Опорные задачи теории групп

Методическая разработка

УДК - 519.4 (07)
ББК - 74.262.6

Опорные задачи теории групп: Методическая разработка. - Челябинск: Издательство "Факел" Челябинского педагогического университета, 1997. - 66 с.

Методическая разработка предназначена для первоначального знакомства с теорией групп. Она содержит систему задач с решениями, ориентированную на усвоение основных понятий теории групп.

Разработка рассчитана на студентов математических факультетов педагогических вузов.

Авторы - составители: Т.В. Ершова, О.Г. Карпушина

Научный редактор: канд. физ.- мат. наук, доцент ЧГПУ В.М. Ситников

Рецензенты: канд. пед. наук, доцент ЧГПУ И.И. Пак;
канд. физ.- мат. наук, доцент ЧелГУ В.Э. Гейт

Предисловие

Изучение темы “Группы” в курсе алгебры всегда вызывает у студентов большие трудности, связанные большей частью с абстрактным характером теории. Но наряду с этим, следует отметить отсутствие или недостаточное распространение пособий, содержащих систему упражнений и задач с полными и подробными решениями, способствующих быстрому пониманию рассматриваемых вопросов. Наша разработка составлена с целью восполнить в какой-то мере этот пробел, помочь студентам при изучении теории групп.

Материал разработки состоит из девяти параграфов. В начале параграфа приводятся необходимые понятия и утверждения теории, а далее решаются задачи, соответствующие рассматриваемым вопросам и расположенные по возрастанию степени сложности. В конце параграфа приведен список аналогичных задач. Их можно использовать для самостоятельного решения, а также при составлении контрольных работ для студентов-заочников.

Авторы разработки не претендуют на оригинальность. Формулировки определений, теорем и задач практически без изменений взяты из пособий, список которых помещен в конце разработки. Более того, каждая задача снабжена ссылкой на литературу. Особо отметим, что авторы ставили цель - выбрать те задачи, которые можно отнести к так называемым типовым задачам, и надеются, что работа по этому пособию подготовит читателя к решению более трудных задач по теории групп.

Авторы считают приятным долгом выразить благодарность всем, кто прочитал рукопись пособия. Высказанные замечания помогли при окончательном редактировании текста.

§1. Бинарные операции и алгебраические системы

Определение 1.1. Бинарной операцией на непустом множестве A называется отображение множества $A \times A$ в A:

$$A \times A \to A,$$

т.е. любой упорядоченной паре (a,b), где $a, b \in A$, сопоставляется только один элемент $c \in A$.

Задачи

1.1. ([8], с.5, №3) Какие из арифметических действий (сложение, вычитание, умножение, деление) являются бинарными операциями:
а) на множестве $A = \{-1; 0; 1\}$;
б) на множестве N;
в) на множестве Z?

Решение.

а) **сложение:** при $a = b = 1$ $a + b \notin A$; **вычитание:** при $a = 1, b = -1$ $a - b \notin A$;

умножение: $\forall a, b \in A \quad ab \in A$. См. таблицу умножения:

·	**-1**	**0**	**1**
-1	1	0	-1
0	0	0	0
1	- 1	0	1

деление: при $a = 1, \ b = 0$ частное a/b не существует.

б) **сложение:** $\forall a, b \in N \quad a + b \in N$;

вычитание: при $a = 3, \ b = 7 \ a - b \notin N$;

умножение: $\forall a, b \in N \quad ab \in N$; **деление:** при $a = 1, \ b = 2 \ a/b \notin N$.

в) **сложение:** $\forall a, b \in Z \quad a + b \in Z$; **вычитание:** $\forall a, b \in Z \quad a - b \in Z$;

умножение: $\forall a, b \in Z \quad ab \in Z$; **деление**: при $a = 1, \ b = 2 \ a/b \notin Z$.

Ответ: а) умножение; б) сложение, умножение; в) сложение, умножение, вычитание.

1.2. ([10], с.83, №8.2) Укажите, какие из следующих операций являются бинарными в трехмерном евклидовом пространстве:
1) умножение вектора на скаляр;
2) скалярное произведение векторов;
3) векторное умножение векторов.

Решение.

1) $\forall \vec{a} \in V_3 \quad \forall \lambda \in R \quad \vec{b} = \lambda \vec{a} = (\lambda x, \lambda y, \lambda z) \in V_3$, но $\lambda \notin V_3$, поэтому операция не является бинарной.

2) $\forall \vec{a}, \vec{b} \in V_3 \quad \vec{a} \cdot \vec{b} = c, c \in R$, поэтому операция не является бинарной.

3) $\forall \vec{a}, \vec{b} \in V_3 \quad [\vec{a}, \vec{b}] \in V_3$, поэтому операция является бинарной.

1.3. ([8], с.6, №6) Является ли деление бинарной операцией на множестве: а) Q; б) R; в) $Q\backslash\{0\}$; г) $R\backslash\{0\}$?

Решение.

а) При $a \neq 0, \ b = 0$ частное a/b не существует. б) Аналогично решению (а).

в) $\forall a, b \in Q\backslash\{0\} \quad a/b \in Q\backslash\{0\}$. г) $\forall a, b \in R\backslash\{0\} \quad a/b \in R\backslash\{0\}$.

Ответ: а) нет; б) нет; в) да; г) да.

1.4. ([8], с.6, №8) Является ли бинарной операцией действие, выполняемое по правилу $a \circ b = a^2 - 2ab + b^2$, на множестве: а) N; б) Z?

Решение.

а) При $a = b = 1 \quad 1 \circ 1 = 1 - 2 + 1 = 0 \notin N$.

б) $\forall a, b \in Z \quad a \circ b = a^2 - 2ab + b^2 \in Z$.

Ответ: а) нет; б) да.

1.5. ([8], с.6, №9) Являются ли действия, выполняемые по следующим формулам, бинарными операциями на множестве Q:

а) $a \circ b \quad (a+b)^2$; б) $a \circ b \quad \dfrac{a+b}{2}$; в) $a \circ b \quad \dfrac{a(a+1)+b(b+1)}{2}$?

Решение.

а) $\forall a, b \in Q \quad a \circ b = (a+b)^2 \in Q$; б) $\forall a, b \in Q \quad a \circ b = \dfrac{a+b}{2} \in Q$;

в) $\forall a, b \in Q \quad a \circ b = \dfrac{a(a+1)+b(b+1)}{2} \in Q$.

Ответ: а) да; б) да; в) да.

1.6. ([8], с.6, №7) Является ли бинарной операцией матричное умножение на множестве:

а) матриц вида $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, где a - любое действительное число;

б) треугольных матриц третьего порядка, т.е. матриц вида

$\begin{pmatrix} a_{11} & 0 & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, где a_{ij} - любые действительные числа?

Решение. а) $M = \left\{ A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in R \right\}$; $\forall A, B \in M \;\; AB \in M$, т.к.

$$AB \;\; \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix};$$

б) $M = \left\{ A = \begin{pmatrix} a_{11} & 0 & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \mid a_{ij} \in R \right\}$; $\forall A, B \in M \;\; AB \in M$, т.к.

$$AB \;\; \begin{pmatrix} a_{11} & 0 & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} b_{11} & 0 & 0 \\ b_{21} & b_{22} & 0 \\ b_{31} & b_{32} & b_{33} \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11}b_{11} & 0 & 0 \\ a_{21}b_{11} + a_{22}b_{21} & a_{22}b_{22} & 0 \\ a_{31}b_{11} + a_{32}b_{21} + a_{33}b_{31} & a_{32}b_{22} + a_{33}b_{32} & a_{33}b_{33} \end{pmatrix}.$$

Ответ: а) да; б) да.

1.7. ([3], с.78, №5) Пусть M - множество радиус-векторов, находящихся в первой четверти координатной плоскости. Будет ли бинарной операцией сложение векторов на множестве M?

Решение. По условию $M = \{(x;y) \mid x \geq 0, y \geq 0\}$;

$\forall \vec{a}, \vec{b} \in M \quad \vec{a} + \vec{b} = (x;y) + (z;t) = (x+z; y+t) \in M,$

так как из того, что $x \geq 0$, $y \geq 0$, $z \geq 0$, $t \geq 0$ следует $x + z \geq 0$, $y + t \geq 0$.

Ответ: да.

Определение 1.2. Алгебраической системой называется непустое множество с набором алгебраических операций и отношений, определенных на нем.

1.8. ([8], с.6, №11) Является ли алгебраической системой множество чисел вида $a + b\sqrt{5}$, где $a, b \in Z$, относительно: а) сложения; б) умножения; в) вычитания?

Решение.

а) $A = \{a + b\sqrt{5} \mid a,b \in Z\}$;

$$\forall a,b\ c,d \in Z \quad (a+b\sqrt{5})+(c+d\sqrt{5}) = (a+c)+(b+d)\sqrt{5} \in A,$$

так как $a + c,\ b + d \in Z$.

б) $\forall a,b\ c,d \in Z \quad (a+b\sqrt{5})(c+d\sqrt{5}) = (ac+5bd)+(ad+bc)\sqrt{5} \in A,$

так как $ac + 5bd,\ ad + bc \in Z$.

в) $\forall a,b\ c,d \in Z \quad (a+b\sqrt{5})-(c+d\sqrt{5}) = (a-c)+(b-d)\sqrt{5} \in A,$

так как $a - c,\ b - d \in Z$.

Ответ: а) да; б) да; в) да.

1.9. ([8], с.6, №12) Является ли алгебраической системой множество радиус-векторов, исходящих из начала координат и расположенных в первой четверти координатной плоскости с операцией: а) сложения векторов; б) вычитания векторов?

Решение.

а) Аналогично решению задачи 1.7. б) При $\vec{a} = (2;3), \vec{b} = (4;5)$

$\vec{a} - \vec{b} = (-2;-3) \notin V$, где $V = \{\vec{a} = (x;y) \mid x \geq 0, y \geq 0\}$.

Ответ: а) да; б) нет.

Дополнительные задачи: [8], с.5, №4; [8], с.5, №5; [8], с.6, №10; [5], с.35, №2.1.1; [8], с.4, №1; [8], с.6, №14.

§2. Коммутативные и ассоциативные операции. Полугруппы

Определение 1.2. Бинарная операция T на множестве G называется коммутативной, если для любых двух элементов a, b из G выполняется равенство $a\mathrm{T}b = b\mathrm{T}a$.

Определение 1.2. Бинарная операция T на множестве G называется ассоциативной, если для любых трех элементов a, b,c из G выполняется равенство $a\mathrm{T}(b\mathrm{T}c) = (a\mathrm{T}b)\mathrm{T}c$.

Замечание 2.1. Напомним, что в поле комплексных чисел и, следовательно, на любом числовом множестве сложение и умножение коммутативные и ассоциативные операции.

Задачи

2.1. ([8], с.8, №2) Является ли коммутативными и ассоциативными на множестве Z бинарные операции сложения; умножения; вычитания?

Решение.

Z - числовое множество, поэтому

$$\forall a,b \in Z \quad a+b=b+a, \quad \forall a,b,c \in Z \quad a\cdot(b+c)=(a+b)+c;$$

$$\forall a,b \in Z \quad ab=ba, \quad \forall a,b,c \in Z \quad a(bc)=(ab)c;$$

но при $a=7, b=2$ $a-b \neq b-a$,

при $a=7, b=4, c=1$ $a-(b-c) \neq (a-b)-c$.

Ответ: сложение и умножение коммутативны и ассоциативны; вычитание - нет.

2.2. Является ли коммутативными и ассоциативными на множестве $Q\backslash\{0\}$ бинарные операции: а) умножения; б) деления?

Решение.

а) Операция умножения коммутативна и ассоциативна (см. замечание 2.1).

б) При $a=5, b=2$ $5/2 \neq 2/5$.

При $a=6, b=2, c=3$ $(6:2):3 \neq 6:(2:3)$.

Операция деления некоммутативна и неассоциативна.

2.3. ([8], с.8, №4) Какие из нижеприведенных бинарных операций

а) $a \circ b = a^b$;

б) $a \circ b = d$, где $d = \text{НОД}(a, b)$;

в) $a \circ b = m$, где $m = \text{НОК}(a, b)$

являются коммутативными и ассоциативными на множестве N?

Решение.

а) При $a=2, b=3$ $2 \circ 3 = 2^3 = 8, 3 \circ 2 = 3^2 = 9, 8 \neq 9$.

$a \circ (b \circ c) = a \circ b^c = a^{b^c}$, $(a \circ b) \circ c = a^b \circ c = a^{bc}$.

При $a=b=2, c=3$ $a^{b^c} \neq a^{bc}$.

Операция $\circ$ некоммутативна и неассоциативна.

б) $\forall a, b \in N$ $a \circ b = b \circ a$ по определению НОД на множестве натуральных чисел.

Кроме того,

$$\forall a, b, c \in N \quad \text{НОД}(\text{НОД}(a, b), c) = \text{НОД}(a, \text{НОД}(b, c)).$$

Операция коммутативна и ассоциативна.

в) Операция коммутативна и ассоциативна по определению НОК.

2.4. ([8], с.8, №5) Докажите, что на множестве R^+ бинарная операция нахождения среднего геометрического $a \circ b = \sqrt{ab}$ коммутативна, но не ассоциативна.

Решение.

1) $\forall\, a, b \in R^+ \;\; a \circ b = \sqrt{ab}$, $b \circ a = \sqrt{ba}$, $\sqrt{ab} = \sqrt{ba}$.

Операция коммутативна.

2) При $a = 2$, $b = c = 3$ $\sqrt{2\sqrt{3 \cdot 3}} = \sqrt{6}$, $\sqrt{\sqrt{2 \cdot 3} \cdot 3} = \sqrt{3\sqrt{6}}$, $\sqrt{6} \neq \sqrt{3\sqrt{6}}$.

Операция неассоциативна.

2.5. ([8], с.8, №6) Почему действие, выполняемое по правилу $a \circ b = a^2 - b^2$, не является бинарной операцией на множестве N? Выясните, коммутативна ли указанная операция на Z; покажите, что она не является ассоциативной на этом множестве.

Решение.

1) При $a = 1$, $b = 3$ $1 \circ 3 = 1^2 - 3^2 = -8 \notin N$. Действие не является бинарной операцией на N.

2) На множестве Z действие является бинарной операцией, т.к.

$$\forall\, a, b \in Z \;\; a \circ b = a^2 - b^2 \in Z.$$

3) При $a = 1$, $b = 2$ $a^2 - b^2 \neq b^2 - a^2$, т.к. $1^2 - 2^2 = -3$, $2^2 - 1^2 = 3$. Операция некоммутативна.

4) При $a = 1$, $b = 2$, $c = 3$ $1^2 - (2^2 - 3^2)^2 = -24$, $(1^2 - 2^2)^2 - 3^2 = 0$, $-24 \neq 0$.

Операция не является ассоциативной.

2.6. ([8], с.9, №9) Покажите, что на некотором множестве, имеющем, по крайней мере, два элемента, бинарная операция, заданная формулой $a \circ b = b$, некоммутативна, но ассоциативна.

Решение.

1) Обозначим множество через A. Пусть $a, b \in A$, $a \neq b$, тогда $a \circ b = b$, $b \circ a = a$. Следовательно, $a \circ b \neq b \circ a$. Операция некоммутативна.

2) $\forall\, a, b, c \in A$. $a \circ (b \circ c) = a \circ c = c$, $(a \circ b) \circ c = b \circ c = c$.

Операция ассоциативна.

2.7. ([10], с.83, №8.1) Определите, какие из операций - сложение, вычитание, умножение, деление - являются бинарными на следующих подмножествах из R: 10) $R \backslash Q$, 11) $\{0\}$, 13) $\{0; 1\}$. Какие из бинарных операций коммутативны, ассоциативны?

Решение.

10) При $a = \sqrt{2}$, $b = -\sqrt{2}$ $a + b = 0 \notin R \backslash Q$.

Сложение не является бинарной операцией.

При $a = b = \sqrt{2}$ $a - b = 0 \notin R\backslash Q$. Вычитание не является бинарной операцией.

При $a = b = \sqrt{2}$ $ab = 2 \notin R\backslash Q$. Умножение не является бинарной операцией.

При $a = b = \sqrt{2}$ $a/b = 1 \notin R\backslash Q$. Деление не является бинарной операцией.

11) Так как $0 + 0 = 0$, $0 - 0 = 0$, $0 \cdot 0 = 0$, $0 : 0 = 0$, то все операции являются бинарными. Очевидно, что они коммутативны и ассоциативны.

13) Сложение и вычитание не являются бинарными операциями, т.к.

$$1+1 = 2 \notin \{0; 1\},\ 0 - 1 = -1 \notin \{0; 1\}.$$

$\forall\, a, b \in \{0; 1\}$ $ab \in \{0; 1\}$, поэтому умножение является бинарной операцией, причем коммутативной, ассоциативной.

При $a = 1$, $b = 0$ частное a/b не существует, деление не является бинарной операцией.

Определение 2.3. Группоидом называется непустое множество с заданной на нем бинарной операцией.

Определение 2.4. Группоид называется полугруппой, если заданная на нем операция ассоциативна.

2.8. ([8], с.8, №8) Покажите, что бинарная операция матричного умножения на множестве матриц вида $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, где $a \in R$, коммутативна и ассоциативна. Является алгебраическая система $(M, \cdot)$ полугруппой?

Решение.

1) $\forall A, B \in M$ $AB = BA$,

так как AB $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+a \\ 0 & 1 \end{pmatrix}$, BA $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$,

поэтому операция коммутативна.

2) $\forall A, B, C \in M$ $A(BC) = (AB)C$, так как

$$A(BC) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\left(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\right) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & c+b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & c+b+a \\ 0 & 1 \end{pmatrix},$$

$$(AB)C = \left(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b+c \\ 0 & 1 \end{pmatrix},$$

поэтому операция ассоциативна и алгебраическая система $(M, \cdot)$ является полугруппой.

2.9. ([8], с.9, №13) Покажите, что множество четырехмерных векторов вида $(a, b, b, 0)$, где $a,b \in N$, образует полугруппу относительно сложения.

Решение.

1) Пусть $V = \{(a, b, b, 0) | \ a,b \in N\}$.

$\forall\ a, b, c, d \in N\ \ (a, b, b, 0) + (c, d, d, 0) = (a + c, b + d, b + d, 0) \in V.$

Следовательно, сложение является бинарной операцией.

2) операция ассоциативна (см. замечание 2.1).

Таким образом, $(V,+)$ - полугруппа.

2.10. ([8], с.9, №12) Покажите, что множество {-1; 0; 1}образует полугруппу относительно обычной операции умножения.

Решение.

1) Пусть G ={-1; 0; 1}. Множество G конечно, поэтому можно расположить произведения двух элементов множества в виде таблицы:

·	**-1**	**0**	**1**
-1	1	0	-1
0	0	0	0
1	-1	0	1

Таблица состоит только из элементов множества G, следовательно, умножение - бинарная операция на G.

2) Умножение, очевидно, ассоциативно, $(G, \cdot)$ - полугруппа.

2.11. ([10], с.83, №8.5) Укажите, какие из следующих подмножеств
1) $A = \{2^n | n \in Z\}$; 2) $A = \{2^n | n = -2; -1; 0; 1; 2\}$; 5) $A = \{z \in C \mid |z| = 1\}$;
6) $A = \{ z \in C \mid |z| \le 1\}$; 15) $A = \{ z \in C \mid |z| = 1/2\}$
множества C с операцией - умножение - являются полугруппами?

Решение.

1) $\forall\ a, b \in Z\ \ 2^a \cdot 2^b = 2^{a+b} \in A$, следовательно, умножение - бинарная операция, причем ассоциативная, и $(A, \cdot)$ - полугруппа.

2) $2 \cdot 2^2 = 2^3 \notin A$, следовательно, операция не является бинарной.

5) $\forall\ a, b \in A\ ab \in A$, т. к. $|ab| = |a||b| = 1 \cdot 1 = 1$. Умножение - бинарная и ассоциативная операция на множестве A, $(A, \cdot)$ - полугруппа.

6) $\forall\ a, b \in A\ ab \in A$, т.к. $|ab| = |a||b| \le 1 \cdot 1 = 1$. Умножение является бинарной ассоциативной операцией на множестве A. $(A, \cdot)$ - полугруппа.

15) $\forall\ a, b \in A\ \ |ab| = |a||b| = (1/2) \cdot (1/2) \neq 1/2$, поэтому $ab \notin A$ и умножение не является бинарной операцией.

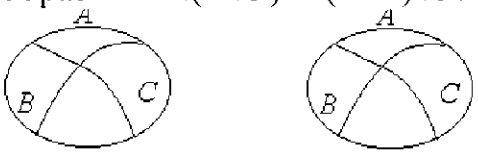
2.12. ([10], с.84, №8.8) Пусть P- множество всех подмножеств данного непустого множества U. Образует ли множество P полугруппу, если на нем задана операция: а) пересечение; б) объединение; в) разность?

Решение.

1) $\forall A,B \in P \quad A \cap B,\ A \cup B,\ A \setminus B \in P$.

Все три операции бинарные. Известно, что операции пересечения и объединения ассоциативны. Следовательно, $(P, \cap)$, $(P, \cup)$ - полугруппы.

2) Пусть $A,B,C \in P$. Изобразим $A\setminus(B\setminus C)$ и $(A\setminus B)\setminus C$:



$A\setminus(B\setminus C)$ $\qquad$ $(A\setminus B)\setminus C$

Из рисунков видно, что $A\setminus(B\setminus C) \neq (A\setminus B)\setminus C$. Следовательно, эта операция неассоциативна.

Дополнительные задачи: [8], с.8, №7; [10], с.83, №8.1 (остальные пункты); [8], с.7, №11; [8], с.9, №10; [8], с.9, №15; [10], с.83, №8.4; [8], с.9, №11; [10], с.83, №8.5 (остальные пункты).

§3. Нейтральные и обратные элементы. Обратимые операции

Определение 3.1. Пусть на множестве G задана бинарная операция T. Говорят, что для операции T существует обратная операция $\perp$, если для любых элементов a, b из G существуют, и притом единственные, элементы x и y из G такие, что выполняются равенства

$$a\mathrm{T}x = b \quad \text{и} \quad y\mathrm{T}a = b.$$

Определение 3.2. Операция T называется обратимой на множестве G, если для неё существует обратная операция.

Определение 3.3. Элемент e из G называется нейтральным элементом относительно операции T, если для любого элемента a из G выполняются равенства: $a\mathrm{T}e = e\mathrm{T}a = a$.

Нейтральный элемент относительно операции сложения называется нулевым элементом или нулем и обозначается θ или 0.

Нейтральный элемент относительно операции умножения называется единичным элементом или единицей и обозначается e или 1.

Теорема 3.1. Если в множестве G существует нейтральный элемент, то он только один.

Доказательство. Действительно, если e_1 и e_2 - два нейтральных элемента, то

$$e_1 = e_1 \mathrm{T} e_2 = e_2.$$

Определение 3.4. Пусть множество G содержит нейтральный элемент e относительно бинарной операции T. Элемент a' из G называется симметричным для элемента $a \in G$, если выполняются равенства: $a\mathrm{T}a' = a'\mathrm{T}a = e$.

Симметричный элемент для элемента a относительно операции сложения называется противоположным элементом и обозначается $-a$.

Симметричный элемент для элемента a относительно операции умножения называется обратным элементом и обозначается a^{-1}.

Теорема 3.2. Если бинарная операция ассоциативна, то никакой элемент не может иметь более одного симметричного.

Доказательство. Пусть a' и a'' - симметричные элементы для элемента a, т.е. $aTa' = a'\mathrm{T}a = e$ и $a\mathrm{T}a'' = a''\mathrm{T}a = e$, тогда

$$a' = a'\mathrm{T}e = a'\mathrm{T}(a\mathrm{T}a'') = (a'\mathrm{T}a)\mathrm{T}a'' = e\mathrm{T}a'' = a''.$$

Теорема 3.3. (Условие обратимости операции.) Ассоциативная операция на множестве A обратима тогда и только тогда, когда в A существует нейтральный элемент и для любого элемента из A существует обратный ему элемент. Доказательство см. в [2].

Задачи

3.1. ([5], с.36, №2.1.8) Докажите, что в алгебре $(N, \circ)$, где $a \circ b = \max\{a, b\}$, существует нейтральный элемент. Укажите все симметризуемые элементы.

Решение. 1) По определению нейтрального элемента $a \circ e = a$, а по условию $a \circ e = \max\{a, e\}$. Таким образом, $a = \max\{a, e\}$ для $\forall\, a \in N$. Последнее соотношение выполняется только при $e = 1$. Следовательно, нейтральный элемент существует.

2) По определению обратного элемента $a \circ x = 1$, по условию $a \circ x = \max\{a, x\}$. Значит, $1 = \max\{a, x\}$. Отсюда следует, что $a = 1$ и $x = 1$. Таким образом, 1 - единственный симметризуемый элемент.

3.2. ([8], с.9, №16) Докажите, что во множестве K, содержащем не менее двух элементов, на котором операция задана формулой $a \circ b = b$, не существует нейтрального элемента.

Решение. Допустим, что существует нейтральный элемент $e \in K$. По определению нейтрального элемента $a \circ e = a$ для $\forall\, a \in K$. По условию $a \circ e = e$,

следовательно, $a = e$. Это значит, что множество K состоит из одного элемента, что противоречит условию задачи. Следовательно, сделанное допущение неверно.

3.3. ([8], с.10, №19) Докажите, что бинарная операция матричного умножения на множестве матриц вида $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, где $a \in R\setminus\{0\}$, обратима. Найдите обратные матрицы для матриц

$$A = \begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix},\ B = \begin{pmatrix} \sqrt{2} & 0 \\ 0 & \sqrt{2} \end{pmatrix},\ C = \begin{pmatrix} 1/3 & 0 \\ 0 & 1/3 \end{pmatrix}.$$

Решение. 1) По определению обратной операции

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix},\quad \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}.$$

Выполнив умножение и приравняв полученные матрицы, получим

$$\begin{pmatrix} ax & 0 \\ 0 & ax \end{pmatrix} = \begin{pmatrix} ya & 0 \\ 0 & ya \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix},$$

откуда $ax = b$, $ya = b$. Тогда $x = y = b/a$. Следовательно, операция обратима. Полагая $b = 1$, получим, что $A^{-1} = \begin{pmatrix} 1/a & 0 \\ 0 & 1/a \end{pmatrix}$.

2) Найдем обратные матрицы для A, B, C:

$$A^{-1} = \begin{pmatrix} -1/2 & 0 \\ 0 & -1/2 \end{pmatrix},\ B^{-1} = \begin{pmatrix} 1/\sqrt{2} & 0 \\ 0 & 1/\sqrt{2} \end{pmatrix},\ C^{-1} = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}.$$

3.4. ([8], с.10, №18) Обладает ли множество чисел вида $a+b\sqrt{5}$, где $a,b \in Z$, нейтральным элементом относительно обычного умножения? Проверьте, имеются ли в данной алгебраической системе обратные элементы для чисел $2+\sqrt{5}$ и $5-2\sqrt{5}$. Обратима ли на данном множестве операция умножения?

Решение. Обозначим данное множество чисел через A.

1) Нейтральным элементом является 1, т.к. $1 = 1+0\sqrt{5}$.

2) По определению обратного элемента $xy = 1$, тогда $y = 1/x$.

Если $x = 2+\sqrt{5}$, то $1/(2+\sqrt{5}) = \dfrac{2-\sqrt{5}}{4-5} = -2+\sqrt{5} \in A$. Значит, для числа $2+\sqrt{5}$ существует обратный элемент из A.

Если же $x = 5-2\sqrt{5}$, то $1/(5-2\sqrt{5}) = \dfrac{5+2\sqrt{5}}{25-20} = 1+\dfrac{2}{5}\sqrt{5} \notin A$.. Значит, для числа $5-2\sqrt{5}$ не существует обратного элемента в данном множестве.

3) Для $5-2\sqrt{5}$ нет обратного в A. Операция не обратима (см. теорему 3.3).

3.5. ([8], с.10, №20) Докажите, что относительно бинарной операции $a \circ b = \frac{a+e}{2}$ множество R не содержит нейтрального элемента. Является ли данная операция обратимой на множестве R?

Решение. 1) Пусть e - нейтральный элемент. По определению нейтрального элемента $a \circ e = a$. По условию $a \circ e = \frac{a+e}{2}$. Тогда $a = \frac{a+e}{2}$,

$$2a = a + e, a = e \text{ для } \forall a \in R.$$

Получили противоречие с единственностью нейтрального элемента.

2) С учетом коммутативности операции $\circ$ и определения обратной операции напишем уравнение $a \circ x = b$; по условию $a \circ x = \frac{a+x}{2}$; тогда $b = \frac{a+x}{2}$, $x = 2b - a \in R$. Следовательно, операция обратима.

3.6. ([8], с.10, №21) Обладает ли множество N правым нейтральным элементом; левым нейтральным; нейтральным элементом относительно бинарной операции, выполняемой по правилу $a \circ b = a^b$? Обратима ли данная операция на множестве N?

Решение. 1) Пусть существует $e \in N$ такой, что $\forall b \in N \quad e \circ b = b$, т.е. $e^b = b$. Полагая $b = 1$, получим $e = 1$. Но при $b = 2$ $1^2 \neq 2$. Следовательно, множество N не обладает левым нейтральным элементом.

$\forall a \in N \quad a \circ 1 = a^1 = a$, следовательно, множество N обладает правым нейтральным элементом. Но так как нет левого нейтрального элемента, то множество N нейтрального элемента не имеет.

2) $\forall a, b \in N \; a \circ x = b$, т.е. $a^x = b$. Решим это уравнение при $a = 1$, $b = 2$: $1^x = 2$. Полученное уравнение не имеет решений, поэтому операция не обратима.

3.7. ([8], с.10, №25) Пусть $\mathfrak{I}$ - множество подмножеств непустого множества M. Существует ли в $\mathfrak{I}$ нейтральный элемент (если существует, то какой) относительно операций: 1) объединения, 2) пересечения подмножеств из $\mathfrak{I}$? Какие элементы из множества $\mathfrak{I}$ имеют обратные? Обратимы ли указанные операции на множестве $\mathfrak{I}$?

Решение. 1) $\mathfrak{I} = \{M_i \mid M_i \subseteq M, M \neq \varnothing, i \in I\}$, I - множество индексов. Рассмотрим множество $\mathfrak{I}$ с ассоциативной операцией объединения. $\forall M_i \in \mathfrak{I}$ $M_i \cup \varnothing = M_i$, значит, пустое множество является нейтральным элементом. Уравнение $M_i \cup X = \varnothing$ разрешимо только для $M_i = \varnothing$. Тогда $X = \varnothing$.

Таким образом, обратный элемент существует только для $\varnothing$; поэтому операция объединения не обратима (см. теорему 3.3).

2) Рассмотрим $(\mathfrak{I}, \cap)$. $\forall\ M_i \in \mathfrak{I}\ M_i \cap M = M_i$, следовательно, M - нейтральный элемент относительно операции пересечения. Уравнение $M_i \cap X = M$ разрешимо только для $M_i = M$. Тогда $X = M$. Обратный элемент существует только для множества M; операция пересечения не обратима.

3.8. ([8], с.11, №26) Докажите, что на множестве Z действие, выполняемое по правилу $a \circ b = \begin{vmatrix} 0 & a \\ b & 0 \end{vmatrix}$, является бинарной коммутативной, ассоциативной, но не обратимой операцией. Обладает ли система $(Z, \circ)$ нейтральным элементом, и если обладает, то каким именно?

Решение. 1) $\forall\ a, b \in Z\ \ a \circ b = \begin{vmatrix} 0 & a \\ b & 0 \end{vmatrix} = -ab \in Z$. Операция бинарная.

2) $\forall\ a, b \in Z\ \ a \circ b = -ab = b \circ a$. Операция коммутативна.

3) $\forall\ a, b, c \in Z\ \ (a \circ b) \circ c = (-ab) \circ c = -(-abc) = abc$,

$a \circ (b \circ c) = a \circ (-bc) = -a(-bc) = abc$.

Операция ассоциативна.

4) Рассмотрим уравнение $a \circ x = b$, т.е. $-ax = b$. При $a = 0$, $b \neq 0$ это уравнение неразрешимо. Операция не обратима.

5) Для нахождения нейтрального элемента решим уравнение $a \circ e = a$, т.е. $-ae = a$, откуда $e = -1$. Число -1 является нейтральным элементом.

Дополнительные задачи: [5], с.36, №2.1.9; [8], с.9, №17; [8], с.10, №22; [8], с.10, №23; [8], с.10, №24; [8], с.11, №27.

§4. Группы. Основные определения

Определение 4.1. Непустое множество G называется группой относительно заданной на нем бинарной операции T, если выполняются следующие условия:

1. операция T ассоциативна;
2. существует в G нейтральный элемент;
3. для каждого элемента из G имеется обратный элемент в G.

Используя условие обратимости операции, можно дать другое определение группы.

Определение 4.2. Непустое множество G называется группой, если определенная на нем операция ассоциативна и обратима.

Иными словами, множество G с ассоциативной операцией T является группой, если для любых элементов $a \in G$ и $b \in G$ каждое из уравнений $a\mathrm{T}x = b$, $y\mathrm{T}a = b$ имеет единственное решение.

Определение 4.3. Если операция коммутативная, то группа называется коммутативной или абелевой.

Задачи

4.1. ([8], с.13, №4) Выясните, какие из нижеприведенных множеств являются группами относительно указанных операций:

а) множество целых чисел относительно вычитания;

б) множество четных чисел относительно умножения;

в) множество целых чисел, кратных любому заданному натуральному числу n, относительно сложения;

г) множество Q^+ относительно умножения;

д) множество Q относительно умножения;

е) множество $Q\backslash\{0\}$относительно умножения;

ж) множество $R\backslash\{0\}$относительно умножения;

з) множество квадратных матриц n-го порядка с действительными элементами относительно сложения; умножения.

Решение. **а)** $(Z, -)$ не является группой, т.к. операция не ассоциативна.

б) $(2Z, \cdot)$ не является группой, т.к. нет нейтрального элемента.

в) Обозначим данное множество $\mathrm{n}Z$.

1) Сложение - бинарная операция, т.к. $\forall\ \mathrm{n}a, \mathrm{n}b \in \mathrm{n}Z\ \ \mathrm{n}a + \mathrm{n}b \in \mathrm{n}Z$.

2) Сложение ассоциативно.

3) Нейтральным элементом является $0 = \mathrm{n}0 \in \mathrm{n}Z$.

4) Для элемента $\mathrm{n}a$ противоположный элемент $-\mathrm{n}a = \mathrm{n}(-a) \in \mathrm{n}Z$.

$(\mathrm{n}Z,+)$ - группа.

г) Q^+ - множество положительных рациональных чисел.

1) Умножение - бинарная операция, т.к. $\forall\ a,b \in Q^+\ \ ab \in Q^+$.

2) Умножение ассоциативно.

3) Нейтральным элементом является $1 \in Q^+$.

4) Для элемента $a \in Q^+$ обратный элемент $1/a \in Q^+$.

$(Q^+, \cdot)$ - группа.

д) $(Q, \cdot)$ не является группой, т.к. для 0 нет обратного элемента.

е) $Q\backslash\{0\}$ - множество рациональных чисел, не равных 0.

1) $\forall\ a,b \in Q\backslash\{0\}\ \ ab \in Q\backslash\{0\}$, значит, умножение является бинарной операцией.

2) Умножение ассоциативно.

3) Число $1 \in Q\backslash\{0\}$ будет нейтральным элементом.

4) $\forall\ a \in Q\backslash\{0\}\ \ 1/a \in Q\backslash\{0\}$.

$(Q\backslash\{0\}, \cdot)$ - группа.

ж) $(R\backslash\{0\}, \cdot)$ - группа (аналогично **е)**).

з) Обозначим данное множество матриц через $M^{n\times n}$.

1) Умножение и сложение - бинарные операции, т.к.

$$\forall\ A, B \in M^{n\times n}\ \ AB \in M^{n\times n},\ A \cdot B \in M^{n\times n}.$$

2) Обе операции ассоциативны.

3) Нулевая матрица и единичная матрица - нейтральные элементы относительно сложения и умножения соответственно.

4) $\forall\ A = (a_{ij}) \in M^{n\times n}\ \exists\ -A = (-a_{ij}) \in M^{n\times n}$, но не для каждой матрицы существует обратная матрица.

$(M^{n\times n}, +)$ - группа, $(M^{n\times n}, \cdot)$ не является группой.

4.2. ([8], с.14, №5) Выясните, является ли группой множество матриц вида $\begin{pmatrix} a & b \\ b & b \end{pmatrix}$, где a и b - любые, не равные одновременно нулю действительные числа, относительно матричного умножения.

Решение.

$$A = \left\{ \begin{pmatrix} a & b \\ b & b \end{pmatrix} \Big| .. a,b \in R, a^2 + b^2 \neq 0 \right\}.$$

Пусть $\begin{pmatrix} a & b \\ b & b \end{pmatrix}, \begin{pmatrix} c & d \\ d & d \end{pmatrix} \in A$, тогда $\begin{pmatrix} a & b \\ b & b \end{pmatrix} \cdot \begin{pmatrix} c & d \\ d & d \end{pmatrix} = \begin{pmatrix} ac+bd & ad+bd \\ bc+bd & bd+bd \end{pmatrix} \notin A.$

Умножение матриц заданного вида не является бинарной операцией.

4.3. ([8], с.14, №7) Докажите, что множество матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, где a и b - любые, не равные одновременно нулю действительные числа, образуют группу относительно матричного умножения.

Решение.

$$M = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \Big| a,b \in R,\ a^2 + b^2 \neq 0 \right\}.$$

1) $\forall A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in M \; AB = \begin{pmatrix} ac-bd & ad+bc \\ -(bc+ad) & -bd+ac \end{pmatrix} \in M,$

т.к. все элементы матрицы AB действительные числа и

$$(ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2) \neq 0.$$

2) Умножение матриц ассоциативно.

3) Единичная матрица $E \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M.$

4) $\forall A \in M \; a^2 + b^2 \neq 0$, значит, $|A| \neq 0$. Следовательно, для любой матрицы A существует обратная матрица A^{-1}. Найдем A^{-1}. Матрица $A^* = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ состоит из алгебраических дополнений к элементам матрицы A. Транспонируем матрицу A^* и обозначим полученную матрицу A^{**}. Таким образом,

$A^{**} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ и $A^{-1} = \frac{1}{|A|}\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, т.е. $\forall A \in M \; \exists A^{-1} \in M$. $(M, \cdot)$ - группа.

4.4. ([9], с.186, №1634) Выясните, образует ли группу каждое из следующих множеств при указанной операции над элементами:

15) корни n-ой степени из 1 (как действительные, так и комплексные) относительно умножения;

17) невырожденные матрицы порядка n с действительными элементами относительно умножения;

18) матрицы порядка n с элементами из Z относительно умножения;

19) матрицы порядка n с целыми элементами и определителем, равным 1, относительно умножения.

Решение.

15) Множество корней n-ой степени из 1 обозначим через $\sqrt[n]{1}$.

а) $\forall \alpha, \beta \in \sqrt[n]{1} \quad \alpha\beta \in \sqrt[n]{1}$, т.к. $(\alpha\beta)^n = \alpha^n\beta^n = 1 \cdot 1 = 1$.

б) Умножение чисел ассоциативно.

в) Нейтральным элементом является $1 \in \sqrt[n]{1}$.

г) $\forall \alpha \in \sqrt[n]{1} \quad 1/\alpha \in \sqrt[n]{1}$, т.к. $(1/\alpha)^n = 1/(\alpha)^n = 1$. $(\sqrt[n]{1}, \cdot)$ - группа.

17) Обозначим заданное множество матриц через $(R^{n\times n})^*$.

а) $\forall A, B \in (R^{n\times n})^* \; AB \in (R^{n\times n})^*$, т.к. $AB \in R^{n\times n}$ и $|AB| = |A| \cdot |B| \neq 0$.

б) Умножение матриц ассоциативно.

в) Матрица $E \in R^{n\times n}$ и $|E| = 1 \neq 0$.

г) Известно, что для любой невырожденной матрицы существует обратная

матрица, также невырожденная.
$((R^{n\times n})^{*}, \cdot)$ - группа.
18) $(Z^{n\times n}, \cdot)$ - не группа, т.к. для некоторых матриц не существует обратного элемента; например, при $n=2$ для $A=\begin{pmatrix}2 & 0\\ 0 & 0\end{pmatrix}$ нет обратного элемента.

19) Пусть $M = \{A \in Z^{n\times n} \mid |A| = 1\}$.
а) $\forall A, B \in M \;\; AB \in M$, т.к. $AB \in Z^{n\times n}$ и $|AB| = |A|\cdot|B| = 1\cdot 1 = 1$.
б) Умножение матриц ассоциативно.
в) Единичная матрица $E \in M$.
г) $\forall\, A \in M \;\; \exists\, A^{-1} \in M \; AA^{-1} = E$. Тогда $|AA^{-1}| = |A|\cdot|A^{-1}| = |E| = 1$. Значит, $|A^{-1}| = 1$. Кроме того, элементы матрицы A^{-1} принадлежат множеству Z, т.к. они получены из алгебраических дополнений к элементам матрицы A делением на определитель матрицы A, причем $|A| = 1$.
$(M, \cdot)$ - группа.

4.5. ([10], с.85, №8.12) Выясните, какие из следующих множеств образуют группу относительно умножения:
3) $A = \{a + b\sqrt{3} \mid a, b \in Z, a^2 + b^2 \neq 0\}$;
4) $A = \{a + b\sqrt{3} \mid a, b \in Q, a^2 + b^2 \neq 0\}$;
5) $A = \{z \in C \mid |z| = 1\}$; 6) $A = \{z \in C \mid |z| \le 1\}$; 18) $A = \{-1; 1\}$.
Решение. 3) $(A, \cdot)$ - не группа, т.к. для некоторых чисел из A не существует обратного элемента. Например, нет обратного элемента для $1 - \sqrt{3}$:

$$(1-\sqrt{3})^{-1} = \frac{1}{1-\sqrt{3}} = \frac{1+\sqrt{3}}{1-3} = -\frac{1}{2} - \frac{1}{2}\sqrt{3} \notin A.$$

4) $(A, \cdot)$ - группа.
а) $\forall\, a,b,c,d \in Q \;\; (a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (cb + ad)\sqrt{3} \in A$, т.к. $ac + 3bd,\ cb + ad \in Q$ и $(ac + 3bd)^2 + (cb + ad)^2 \neq 0$.
(Если предположить противное, что $ac + 3bd = 0$ и $cb + ad = 0$, то рассмотрение случаев: хотя бы один из элементов a,b,c,d равен нулю или все элементы a,b,c,d отличны от нуля - приводит к противоречию.)
б) Умножение чисел ассоциативно.
в) Число $1 = 1 + 0\cdot\sqrt{3} \in A$.
г) $\forall\, a,b \in Q \quad \dfrac{1}{a+b\sqrt{3}} = \dfrac{a-b\sqrt{3}}{a^2-3b^2} = \dfrac{a}{a^2-3b^2} - \dfrac{b}{a^2-3b^2}\sqrt{3} \in A$, т.к.
$a^2 - 3b^2 \neq 0$ для $a,b \in Q$ и не равных одновременно нулю.
5) Задано множество A комплексных чисел с модулем 1.

а) $(A,\cdot)$ - полугруппа (см. задачу 2.11 п.5).

б) $\forall\, z \in A \quad \frac{1}{z} \in A$, т.к. $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$.

$(A,\cdot)$ - группа.

6) $(A,\cdot)$ - не группа, т.к. для некоторых элементов z из $A \quad \frac{1}{z} \notin A$. Например, для $z = 0{,}1 \quad \frac{1}{z} = 10 \notin A$.

18) Заметим, что $A = \sqrt{1}$. Ввиду задачи 4.4.15 $(A,\cdot)$ - группа .

4.6. ([8], с.16, №20) На множестве $Q\backslash\{0\}$ определено действие

$$a \circ b = (ab)/2.$$

Докажите, что относительно указанного действия данное множество образует группу.

Решение.

1) $\forall\, a,b \in Q\backslash\{0\}\ a \circ b = (ab)/2 \in Q\backslash\{0\}$, поэтому операция бинарная.

2) Умножение ассоциативно.

3) Единичным элементом является число 2, т.к. для любого $a \in Q\backslash\{0\}$ $a \circ 2 = (a2)/2 = a$ (отметим коммутативность операции).

4) $\forall\, a \in Q\backslash\{0\}$ существует обратный элемент $a' = \frac{4}{a} \in Q\backslash\{0\}$.

Действительно, $a \circ \frac{4}{a} = \frac{a \cdot \overset{4}{a}}{2} = 2$. $(Q\backslash\{0\}, \circ)$ - группа.

Определение 4.4. Назовем группу мультипликативной (аддитивной), если операция называется умножением (сложением).

4.7. ([10], с.85, №8.14) Докажите, что следующее множество чисел образует аддитивную группу: $A = \{a + bi\sqrt{3} \mid a, b \in Z\}$.

Решение.

а) $\forall\, a,b,c,d \in Z\ (a + bi\sqrt{3}) + (c + di\sqrt{3}) = (a + c) + (b + d)i\sqrt{3} \in A$, т.к. $a + c,\ b + d \in Z$.

б) Умножение чисел ассоциативно.

в) $0 = 0 + 0i\sqrt{3} \in A$.

г) $\forall\ (a + bi\sqrt{3}) \in A \quad (-a - bi\sqrt{3}) \in A$.

$(A,\cdot)$ - группа.

4.8. ([8], с.16, №22) Пусть $aa = e$ для любого элемента мультипли-

кативной группы G. Докажите, что группа является абелевой.

Решение.

1) По условию $aa = e$, следовательно, $a^{-1} = a$ для любого элемента a из G.

2) Пусть $b,c \in G$. Тогда $(bc)^{-1} = bc$, но $(bc)^{-1} = c^{-1}b^{-1}$. Значит, $bc = cb$ для любых $b,c \in G$. Группа G абелева.

4.9. ([10], с.86, №8.20) Докажите, что следующие множества квадратных матриц второго порядка являются мультипликативными группами:

3) $M = \left\{ \begin{pmatrix} a & -3b \\ b & a \end{pmatrix} \mid a,b \in Q,\ a^2 + b^2 > 0 \right\}$; 4) $M = \left\{ \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \mid \varphi \in R \right\}$.

Решение.

3) а) Если $A - \begin{pmatrix} a & -3b \\ b & a \end{pmatrix}$, $B - \begin{pmatrix} c & -3d \\ d & c \end{pmatrix}$, то $AB - \begin{pmatrix} ac - 3bd & -3(ad + bc) \\ bc + ad & ac - 3bd \end{pmatrix}$.

Кроме того, $(ac - 3bd)^2 + (ad + bc)^2 > 0$. Иначе, $ac - 3bd = 0$, $ad + bc = 0$, откуда получим $\left(\frac{c}{d}\right)^2 = -3$ $(a \neq 0,\ b \neq 0,\ c \neq 0,\ d \neq 0)$, что неверно, т.к. $c, d \in Q$.

б) Умножение матриц ассоциативно.

в) Матрица $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M$, т.к. $1^2 + 0^2 > 0$.

г) $\forall\ A \in M\ \ A^{-1} = \frac{1}{a^2 + 3b^2} \begin{pmatrix} a & 3b \\ -b & a \end{pmatrix} \in M$. $(M, \cdot)$ - группа.

4) а) $\forall\ A = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$, $B = \begin{pmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{pmatrix} \in M\ AB \in M$, т.к.

$$AB = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \begin{pmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{pmatrix} = \begin{pmatrix} \cos(\varphi + \psi) & -\sin(\varphi + \psi) \\ \sin(\varphi + \psi) & \cos(\varphi + \psi) \end{pmatrix}.$$

б) Умножение матриц ассоциативно.

в) $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{pmatrix} \in M$.

г) $\forall\ A \in M\ A^{-1} = \frac{1}{\cos^2\varphi + \sin^2\varphi} \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} = \begin{pmatrix} \cos(-\varphi) & -\sin(-\varphi) \\ \sin(-\varphi) & \cos(-\varphi) \end{pmatrix} \in M$.

$(M, \cdot)$ - группа.

Пусть G - произвольная мультипликативная группа. Для полного задания

группы необходимо знать, чему равны всевозможные попарные произведения, т.е. произведения g_ig_j . В случае конечной группы такие произведения можно задать следующим образом: составляется таблица из n строк и n столбцов; таблица снабжена заглавным столбцом и заглавной строкой, в которых записаны элементы группы в определенном порядке; в клетках таблицы размещаются элементы, равные произведениям g_ig_j. Эта таблица называется таблицей Кэли или таблицей умножения.

Заметим, что таблица Кэли позволяет: находить **нейтральный элемент;** для каждого элемента находить **симметричный**; выяснить, является ли операция **ассоциативной** (для этого по таблице находят соответствующие произведения и проверяют истинность соответствующего равенства; обычно проверка ассоциативности является громоздкой и её стараются избежать при анализе таблицы); определить, является ли операция **коммутативной** (таблица должна быть симметричной относительно главной диагонали).

По таблице Кэли можно определить, является ли данное множество группой в соответствии с определениями 4.1 и 4.2. Таблица Кэли с ассоциативной операцией задает группу тогда и только тогда, когда каждое из уравнений

$$g_ix = g_j,\ yg_i = g_j$$

имеет, и притом единственное, решение. Последнее выполняется тогда и только тогда, когда в каждом столбце и в каждой строке таблицы любой элемент множества встречается только один раз.

4.10. ([10], с.86, №8.18) Докажите, что каждое из следующих множеств с операцией, заданной таблицей, является группой:

1) $A = \{e, a\}$,

$\cdot$	$\boldsymbol{e}$	$\boldsymbol{a}$
$\boldsymbol{e}$	e	a
$\boldsymbol{a}$	a	e

2) $A = \{e, a, b\}$,

$\cdot$	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{b}$
$\boldsymbol{e}$	e	a	b
$\boldsymbol{a}$	a	b	e
$\boldsymbol{b}$	b	e	a

Решение.

1) а) Из таблицы видно, что операция является бинарной.

б) Операция ассоциативна, т.к.

$(aa)e = ee = e$ и $a(ae) = aa = e$; $(ae)a = aa = e$ и $a(ea) = aa = e$;

$(ea)a = aa = e$ и $e(aa) = ee = e$; $(aa)a = ea = a$ и $a(aa) = ae = a$;

$(ee)e = ee = e$ и $e(ee) = ee = e$; $(ae)e = ae = a$ и $a(ee) = ae = a$;

$(ea)e = ae = e$ и $e(ae) = ea = a$; $(ee)a = ea = a$ и $e(ea) = ea = a$.

в) Единичным элементом является e.

г) Для e симметричным является e, элемент a также симметричен себе.

$(A, \cdot)$ - группа.

2) а) Операция является бинарной, что видно по таблице Кэли.

б) Проверка ассоциативности выполняется аналогично пункту 1 б).

в) Единичный элемент - e.

г) Каждый элемент симметричен себе. $(A, \cdot)$ - группа.

Рассмотрим важный класс групп - групп преобразований. Пусть M - некоторое множество. Будем рассматривать всевозможные преобразования множества M, т.е. взаимно однозначные отображения множества M на себя. Обозначим множество этих преобразований через F и определим операцию умножения на F следующим образом: любым двум преобразованиям f и g сопоставим отображение, которое получается в результате последовательного выполнения этих преобразований - сначала преобразования g, а затем преобразования f, т.е. $(fg)(x) = f(g(x))$ для всех x из M. Подчеркнем, что отображение fg преобразований f и g является преобразованием.

Определение 4.5. Композицией или произведением преобразований f и g множества M называется их последовательное выполнение, т.е. $(fg)(x) = f(g(x))$ для всех x из M.

Множество всех взаимно однозначных преобразований непустого множества образует группу относительно умножения преобразований. Действительно, легко проверить, что для любых f, g, h $(fg)h = f(gh)$, тождественное ото-

отображение $\varepsilon : x \to x$ является единичным элементом, т.е. $f\varepsilon = \varepsilon f = f$, и любое преобразование f имеет обратное преобразование f^{-1}.

4.11. ([8], с.12, №3) Пусть G - совокупность всех преобразований множества R, задаваемых формулой $f(x) = x + a$, где $a \in R$. Докажите, что G - группа относительно умножения преобразований. Укажите нейтральный элемент этой группы и для каждого элемента найдите обратный.

Решение.

1) Пусть $G = \{f \mid f(x) = x \cdot a, a \in R\}$.

$\forall f(x) = x \cdot a, g(x) = x \cdot b \in G \quad fg \in G$, т.к.

$$(fg)(x) = f(g(x)) = f(x + b) = x - b + a.$$

Операция является бинарной.

2) Умножение преобразований ассоциативно.

3) Тождественное преобразование ε такое, что $\varepsilon(x) = x \cdot 0$, является единицей. Действительно, $\forall f \in G \; f\varepsilon = \varepsilon f = f$, т.к.

$(f\varepsilon)(x) = f(\varepsilon(x)) = f(x) = x \cdot a$ и $(\varepsilon f)(x) = \varepsilon(f(x)) = \varepsilon(x \cdot a) = x \cdot a$.

4) $\forall f \in G \; \exists f^{-1} \in G$. В самом деле, пусть $f^{-1}(x) = x - a$, тогда

$$(ff^{-1})(x) = f(x - a) = (x - a) + a = x \quad \text{и}$$
$$(f^{-1}f)(x) = f^{-1}(x + a) = (x - a) - a = x\text{, т.е. } ff^{-1} = f^{-1}f = \varepsilon\text{.}$$

Итак, $(G, \cdot)$ - группа; $\varepsilon(x) = x \cdot 0$ - нейтральный элемент; для $f(x) = x - a$ обратный элемент - преобразование $f^{-1}(x) = x - a$.

4.12. ([8], с.26, №3) Докажите, что множество

$$F = \{ f_1(x) = x,\ f_2(x) = -x,\ f_3(x) = 1/x,\ f_4(x) = -1/x \}$$

вещественных функций, заданных на $R \setminus \{0\}$, является группой относительно операции умножения преобразований.

Решение. 1) $\forall f_i \in F\ (i = 1, 2, 3, 4)\quad f_i f_1 = f_1 f_i = f_i$.

Кроме того, а) $f_2 f_2(x) = f_2(f_2(x)) = f_2(-x) = x = f_1(x)$,

$$f_2 f_3(x) = f_2(f_3(x)) = f_2(1/x) = -1/x = f_4(x),$$

$$f_2 f_4(x) = f_2(f_4(x)) = f_2(-1/x) = 1/x = f_3(x);$$

б) $f_3 f_2(x) = f_3(f_2(x)) = f_3(-x) = -1/x = f_4(x)$,

$$f_3 f_3(x) = f_3(f_3(x)) = f_3(1/x) = x = f_1(x),$$

$$f_3 f_4(x) = f_3(f_4(x)) = f_3(-1/x) = -x = f_2(x);$$

в) $f_4 f_2(x) = f_4(f_2(x)) = f_4(-x) = 1/x = f_3(x)$,

$$f_4 f_3(x) = f_4(f_3(x)) = f_4(1/x) = -x = f_2(x),$$

$$f_4 f_4(x) = f_4(f_4(x)) = f_4(-1/x) = x = f_1(x).$$

Составим таблицу Кэли.

Таблица состоит только из элементов множества F, значит, операция бинарная.

2) Умножение преобразований ассоциативно.

3) Единичным элементом является преобразование f_1.

4) Для каждого элемента обратный совпадает с ним.

$\cdot$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

$(F, \cdot)$ - группа.

4.13. ([8], с.27, №5) На множестве M бинарная операция задана таблицей.

Выясните, обладает ли множество M нейтральным элементом относительно заданной бинарной операции,
является ли заданная операция коммутативной, ассоциативной и обратимой. Является ли M полугруппой группой?

$\cdot$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

Решение.

1) b - нейтральный элемент, т.к. $\forall\, x \in M \quad xb = bx = x.$

2) Операция коммутативная, поскольку таблица симметрична относительно главной диагонали.

3) Операция ассоциативна, т.к.

$(aa)a = aa = a$ и $a(aa) = aa = a$; $(aa)b = ab = a$ и $a(ab) = aa = a$;

$(ab)a = aa = a$ и $a(ba) = aa = a$; $(ba)a = aa = a$ и $b(aa) = ba = a.$

Аналогично проверяется соответствующее равенство для aac, aca, caa и других произведений (их всего 27).

4) Операция не является обратимой, т.к. в первой строке и в первом столбце таблицы присутствует только элемент a.

Следовательно, множество M с заданной на нем операцией является полугруппой, но не является группой.

Определение 4.6. Если множество M конечно и состоит из n элементов, то всевозможные отображения множества M на себя называются подстановками, а соответствующая группа преобразований называется симметрической группой n - ой степени или группой подстановок из n элементов. Она обозначается S_n.

Определение 4.7. Подстановка называется четной, если четности верхней и нижней строк совпадают (сумма числа инверсий верхней и нижней строк является четным числом), в противном случае подстановка называется нечетной.

Напомним, что умножение подстановок будем производить по следующему правилу: сначала выполняем правое отображение, затем левое.

Рассмотрим задачу которую в дальнейшем будем часто использовать при решении других задач.

Задача . Для симметрической группы S_3 третьей степени составьте таблицу Кэли.

Решение. Пусть $S_3 = \{p_0,\ p_1,\ p_2,\ p_3,\ p_4,\ p_5\}$, где

$$p_0 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ p_1 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\ p_2 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ p_3 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\ p_4 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ p_5 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}.$$

Найдем всевозможные произведения $p_i p_j$, где $i, j = 0,1,2,3,4,5$.

1) Очевидно, что $\forall\, p_i \in S_3 \quad p_i p_0 = p_0 p_i = p_i$.

2) $p_1 p_1 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = p_2, \quad p_1 p_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = p_0,$

$$p_1p_3=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=p_5,\quad p_1p_4=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=p_3,$$

$$p_1p_5=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=p_4.$$

3) Аналогично найдем, что

$p_2p_1=p_0,\ p_2p_2=p_1,\ p_2p_3=p_4,\ p_2p_4=p_5,\ p_2p_5=p_3$ и т. д.

Составим таблицу Кэли группы S_3:

$\cdot$	$\boldsymbol{p_0}$	$\boldsymbol{p_1}$	$\boldsymbol{p_2}$	$\boldsymbol{p_3}$	$\boldsymbol{p_4}$	$\boldsymbol{p_5}$
$\boldsymbol{p_0}$	p_0	p_1	p_2	p_3	p_4	p_5
$\boldsymbol{p_1}$	p_1	p_2	p_0	p_5	p_3	p_4
$\boldsymbol{p_2}$	p_2	p_0	p_1	p_4	p_5	p_3
$\boldsymbol{p_3}$	p_3	p_4	p_5	p_0	p_1	p_2
$\boldsymbol{p_4}$	p_4	p_5	p_3	p_2	p_0	p_1
$\boldsymbol{p_5}$	p_5	p_3	p_4	p_1	p_2	p_0

Отметим, что группа некоммутативная, т.к. $p_2p_3=p_5$, а $p_3p_2=p_4$.

4.14. ([8], с.14, №10) Для множества $G_1=\{p_0,\ p_1,\ p_2,\ p_3\}$ составьте таблицу умножения, если

$$p_0=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\ p_1=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\ p_2=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\ p_3=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}.$$

С помощью таблицы убедитесь, что G_1 - абелева группа.

Решение. 1) Найдем всевозможные произведения элементов множества G_1.

а) Очевидно, что $\forall\, p_i\in G_1\ \ p_ip_0=p_0p_i=p_i$.

б) Находим произведения $p_1p_1=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=p_2,$

$p_1p_2=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}=p_3,\ \ p_1p_3=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=p_0$

и т.д. Составим таблицу умножения:

$\cdot$	$\boldsymbol{p_0}$	$\boldsymbol{p_1}$	$\boldsymbol{p_2}$	$\boldsymbol{p_3}$
$\boldsymbol{p_0}$	p_0	p_1	p_2	p_3
$\boldsymbol{p_1}$	p_1	p_2	p_3	p_0
$\boldsymbol{p_2}$	p_2	p_3	p_0	p_1
$\boldsymbol{p_3}$	p_3	p_0	p_1	p_2

$(G_1\ ,\cdot)$ - группа, т.к. а) таблица умножения состоит только из элементов множества G_1, значит, операция бинарная; б) операция ассоциативная (умножение преобразований ассоциативно);

в) операция обратима, т.к. в каждом столбце и в каждой строке таблицы присутствуют все элементы множества G_1.

2) Таблица Кэли симметрична относительно главной диагонали; следовательно, группа $(G_1, \cdot)$ абелева.

4.15. ([8], с.15, №12) Дано множество $M = \{a_0, a_1, a_2\}$ поворотов (вращений) правильного треугольника в плоскости этого треугольника вокруг его центра против часовой стрелки соответственно на углы 0°, 120°, 240°. Эти повороты совмещают треугольник с самим собой. Последовательное выполнение двух любых таких поворотов называется произведением (композицией) поворотов. Докажите, что M является группой относительно введенной в M операции.

Решение. $M = \{a_0, a_1, a_2\}$. 1) Обозначим вершины треугольника цифрами 1, 2, 3. Тогда $a_0 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $a_1 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, $a_2 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$.

3 — 120° — 1 — 2

2) Найдем все попарные произведения элементов множества. Ясно, что $\forall\, a_i \in M \quad a_i a_0 = a_0 a_i = a_i$.

$$a_1 a_1 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = a_2,$$

$$a_1 a_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = a_0,.$$

$$a_2 a_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = a_0,\ a_2 a_2 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = a_1.$$

Составим таблицу умножения:

$\cdot$	a_0	a_1	a_2
a_0	a_0	a_1	a_2
a_1	a_1	a_2	a_0
a_2	a_2	a_0	a_1

По таблице видно, что система $(M, \cdot)$ является группой.

Эта группа называется группой поворотов треугольника. Любое преобразование некоторой фигуры в себя, сохраняющее расстояние между её точками, называется **самосовмещением** данной фигуры. Следовательно, повороты являются также и самосовмещениями правильного треугольника.

4.16. ([8], с.15, №13) Кроме поворотов, у правильного треугольника имеется ещё три самосовмещения, а именно, отражения a_3, a_4, a_5 этого треугольника относительно его осей l_1, l_2, l_3 симметрии. Каждое из шести преобразований, переводящих треугольник в себя, можно записать в виде подстановки, где в верхней строке указаны вершины треугольника, а нижняя

строка показывает, во что каждая из них переходит. Пользуясь правилом умножения подстановок, составьте таблицу умножения для всех самосовмещений правильного треугольника и по таблице убедитесь в том, что они составляют группу.

Решение. $M = \{a_0, a_1, a_2, a_3, a_4, a_5\}$, где a_3 - это отражение треугольника относительно оси l_1, a_4 - относительно оси l_2, a_5 - относительно оси l_3.

3

1 _____ 2

$$a_0 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ a_1 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\ a_2 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},$$

$$a_3 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\ a_4 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ a_5 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}.$$

Если заменить буквы a_i на p_i, то получим множество, совпадающее с множеством подстановок третьей степени S_3, которое образует группу относительно умножения подстановок. Следовательно, M - группа относительно умножения преобразований.

Таблица Кэли для этой группы:

$\cdot$	a_0	a_1	a_2	a_3	a_4	a_5
a_0	a_0	a_1	a_2	a_3	a_4	a_5
a_1	a_1	a_2	a_0	a_5	a_3	a_4
a_2	a_2	a_0	a_1	a_4	a_5	a_3
a_3	a_3	a_4	a_5	a_0	a_1	a_2
a_4	a_4	a_5	a_3	a_2	a_0	a_1
a_5	a_5	a_3	a_4	a_1	a_2	a_0

Очевидно, таблица умножения для этой группы совпадает с таблицей Кэли для симметрической группы S_3.

4.17. ([8], с.16, №15) Найдите группу самосовмещений прямоугольника, не являющегося квадратом.

Решение. 1) Обозначим вершины прямоугольника 1, 2, 3, 4.

Пусть M - множество самосовмещений прямоугольника: $M = \{e, a, b, c\}$, где e, a - повороты прямоугольника вокруг центра на 0°, 180° соответственно; b, c - отражения прямоугольника относительно его

осей l_1, l_2 симметрии; $e = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$, $a = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$, $b = \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$, $c = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$.

2) Найдем все попарные произведения элементов e, a, b, c.

а) $\forall x \in M \quad xe = ex = a$.

б) $aa = \begin{pmatrix}1234\\3412\end{pmatrix}\begin{pmatrix}1234\\3412\end{pmatrix} = \begin{pmatrix}1234\\1234\end{pmatrix} = e,\ ab = c,\ ba = c,\ \ ac = b,\ bb = e,$

$bc = a,\ ca = b,\ cb = a,\ cc = e.$

3) Составим таблицу Кэли:

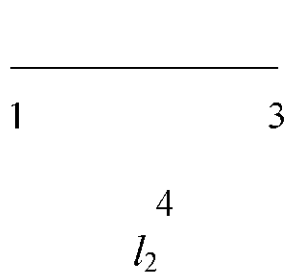
$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Таблица состоит только из элементов множества M, значит, операция бинарная. Кроме того, операция ассоциативная и обратимая, т.к. в каждой строке и в каждом столбце присутствуют все элементы множества M.

Следовательно, M образует группу самосовмещений прямоугольника.

4.18. ([8], с.16, №16) Найдите группу самосовмещений ромба, не являющегося квадратом.

Решение. 1) Обозначим вершины ромба 1, 2, 3, 4. Пусть $M = \{e, a, b, c\}$, где e, a - повороты ромба вокруг центра соответственно на 0^0, 180^0; b, c - отражения ромба относительно его осей l_1, l_2 симметрии;



$e = \begin{pmatrix}1234\\1234\end{pmatrix}, a = \begin{pmatrix}1234\\3412\end{pmatrix}, b = \begin{pmatrix}1234\\1432\end{pmatrix}, c = \begin{pmatrix}1234\\3214\end{pmatrix}.$

2) Найдем все попарные произведения элементов e, a, b, c.

а) $\forall x \in M \quad xe = ex = x.$

б) $aa = \begin{pmatrix}1234\\3412\end{pmatrix}\begin{pmatrix}1234\\3412\end{pmatrix} = \begin{pmatrix}1234\\1234\end{pmatrix} = e,\ ab = c,\ ac = b.$

Остальные произведения находим аналогично.

3) Составим таблицу Кэли:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Из таблицы видно, что операция бинарная, ассоциативная и обратимая. Множество M образует группу самосовмещений ромба.

4.19. ([8], с.28, №7) По таблице Кэли для группы самосовмещений ромба найдите взаимно обратные элементы и выясните, коммутативна ли данная группа.

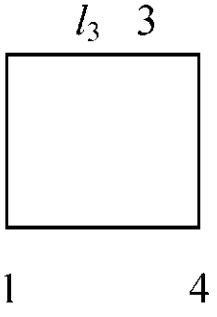
Решение. Взаимно обратных элементов нет. Каждый элемент обратен самому себе. Группа самосовмещений ромба является коммутативной, т.к. таблица симметрична относительно главной диагонали.

4.20. ([8], с.16, №17) Найдите группу самосовмещений квадрата.

Решение.

1) Обозначим вершины квадрата 1, 2, 3, 4.

Пусть $M = \{a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$, где a_0, a_1, a_2, a_3 - повороты квадрата вокруг центра по часовой стрелке соответственно на $0^\circ, 90^\circ, 180^\circ, 270^\circ$; a_4, a_5, a_6, a_7 - отражения квадрата относительно его осей l_1, l_2, l_3, l_4 симметрии.



$a_0 = \begin{pmatrix}1234\\1234\end{pmatrix}$, $a_1 = \begin{pmatrix}1234\\4123\end{pmatrix}$, $a_2 = \begin{pmatrix}1234\\3412\end{pmatrix}$, $a_3 = \begin{pmatrix}1234\\2341\end{pmatrix}$,

$a_4 = \begin{pmatrix}1234\\2143\end{pmatrix}$, $a_5 = \begin{pmatrix}1234\\1432\end{pmatrix}$, $a_6 = \begin{pmatrix}1234\\4321\end{pmatrix}$, $a_7 = \begin{pmatrix}1234\\3214\end{pmatrix}$.

2) Найдем все попарные произведения элементов множества M.

$\forall\, a_i \in M \quad a_i a_0 = a_0 a_i = a_i$; $a_1 a_1 = \begin{pmatrix}1234\\4123\end{pmatrix}\begin{pmatrix}1234\\4123\end{pmatrix} = \begin{pmatrix}1234\\3412\end{pmatrix} = a_2$ и т.д.

3) Составим таблицу Кэли.

$\cdot$	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7
a_0	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7
a_1	a_1	a_2	a_3	a_0	a_5	a_6	a_7	a_4
a_2	a_2	a_3	a_0	a_1	a_6	a_7	a_4	a_5
a_3	a_3	a_0	a_1	a_2	a_7	a_4	a_5	a_6
a_4	a_4	a_7	a_6	a_5	a_0	a_3	a_2	a_1
a_5	a_5	a_4	a_7	a_6	a_1	a_0	a_3	a_2
a_6	a_6	a_5	a_4	a_7	a_2	a_1	a_0	a_3
a_7	a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0

Из таблицы видно, что множество M образует группу.

4.21. ([8], с.15, №11) Докажите, что:

1) при умножении двух подстановок одинаковой четности получается четная подстановка, а при умножении двух подстановок разной четности - нечетная подстановка;
2) подстановки a и a^{-1} имеют одинаковую четность, где a - произвольная подстановка;
3) множество четных подстановок n-ой степени образует группу относительно операции умножения подстановок.

Решение. 1) Пусть $f = \begin{pmatrix} \alpha_1 \dots \alpha_n \\ \beta_1 \dots \beta_n \end{pmatrix}$, $g = \begin{pmatrix} \beta_1 \dots \beta_n \\ \gamma_1 \dots \gamma_n \end{pmatrix}$.

а) Предположим, что f и g - четные подстановки.
$(\alpha_1, \dots, \alpha_n)$ - четная перестановка. Из четности f следует, что $(\beta_1, \dots, \beta_n)$ - четная перестановка. С учетом того, что g - четная подстановка, получим: перестановка $(\gamma_1, \dots, \gamma_n)$ - четная. Тогда

$$gf = \begin{pmatrix} \beta_1 \dots \beta_n \\ \gamma_1 \dots \gamma_n \end{pmatrix} \begin{pmatrix} \alpha_1 \dots \alpha_n \\ \beta_1 \dots \beta_n \end{pmatrix} = \begin{pmatrix} \alpha_1 \dots \alpha_n \\ \gamma_1 \dots \gamma_n \end{pmatrix}$$

будет четной подстановкой.

Аналогично рассматривается случай нечетной перестановки $(\alpha_1, \dots, \alpha_n)$.
б) Пусть f и g - нечетные подстановки. Также, как и в а), рассматриваем случаи четной и нечетной перестановки $(\alpha_1, \dots, \alpha_n)$.
в) Пусть f - четная, g - нечетная подстановка. Дальнейшее очевидно.
г) Пусть f - нечетная подстановка, g - четная подстановка. Дальнейшее очевидно.

2) Пусть $a = \begin{pmatrix} \alpha_1 \dots \alpha_n \\ \beta_1 \dots \beta_n \end{pmatrix}$, тогда $a^{-1} = \begin{pmatrix} \beta_1 \dots \beta_n \\ \alpha_1 \dots \alpha_n \end{pmatrix}$.

Утверждение легко следует из определения четности подстановки.
3) Обозначим данное множество через A_n.
а) $\forall a, b \in A_n \quad ab \in A_n$ (см. пункт 1)).
б) $\forall a, b, c \in A_n \quad (ab)c = a(bc)$.
в) $e = \begin{pmatrix} 12 \dots n \\ 12 \dots n \end{pmatrix} \in A_n$, т.к. e - четная подстановка.
г) $\forall a \in A_n \quad a^{-1} \in A_n$ (см. пункт 2)).

Таким образом, $(A_n, \cdot)$ - группа.

Определение 4.8. Группа всех четных подстановок n -ой степени называется знакопеременной группой n-ой степени и обозначается

через A_n.

4.22. ([10], с.87, №8.23) Решите уравнение $fu = g$, где

$$f = \begin{pmatrix}123456\\251643\end{pmatrix},\ g = \begin{pmatrix}123456\\351642\end{pmatrix}.$$

Решение. Если $fu = g$, то $u = f^{-1}g$.

$$u = \begin{pmatrix}251643\\123456\end{pmatrix}\begin{pmatrix}123456\\351642\end{pmatrix} = \begin{pmatrix}123456\\623451\end{pmatrix}.$$

4.23. ([10], с.87, №8.25) Решите уравнение $fug = h$ при

$$f = \begin{pmatrix}12345\\53124\end{pmatrix},\ g = \begin{pmatrix}12345\\42513\end{pmatrix},\ h = \begin{pmatrix}12345\\54321\end{pmatrix}.$$

Решение. Если $fug = h$, то $u = f^{-1}hg^{-1}$.

$$u = \begin{pmatrix}53124\\12345\end{pmatrix}\begin{pmatrix}12345\\54321\end{pmatrix}\begin{pmatrix}42513\\12345\end{pmatrix} = \begin{pmatrix}53124\\12345\end{pmatrix}\begin{pmatrix}12345\\24153\end{pmatrix} = \begin{pmatrix}12345\\45312\end{pmatrix}.$$

4.24. ([4], с.151, №8.2.15) Разложите в произведение независимых циклов следующие подстановки: а) $\begin{pmatrix}12345\\24513\end{pmatrix}$, $\begin{pmatrix}12345\\45312\end{pmatrix}$, $\begin{pmatrix}12345\\21345\end{pmatrix}$;

б) $\begin{pmatrix}1234567\\7316542\end{pmatrix}$, $\begin{pmatrix}1234567\\2574613\end{pmatrix}$, $\begin{pmatrix}1234567\\1657243\end{pmatrix}$; в) $\begin{pmatrix}123456789\\315692874\end{pmatrix}$, $\begin{pmatrix}123456789\\987654321\end{pmatrix}$.

Решение.

а) $\begin{pmatrix}12345\\24513\end{pmatrix} = (124)(35)$, $\begin{pmatrix}12345\\45312\end{pmatrix} = (14)(25)$, $\begin{pmatrix}12345\\21345\end{pmatrix} = (12)$;

б) $\begin{pmatrix}1234567\\7316542\end{pmatrix} = (1723)(46)$, $\begin{pmatrix}1234567\\2574613\end{pmatrix} = (1256)(37)(56)$, $\begin{pmatrix}1234567\\1657243\end{pmatrix} = (264735)$;

в) $\begin{pmatrix}123456789\\315692874\end{pmatrix} = (1359462)(78)$, $\begin{pmatrix}123456789\\987654321\end{pmatrix} = (19)(28)(37)(46)$.

4.25. ([8], с.22, №16) Следующие элементы симметрической группы S_8, заданные разложением на независимые циклы, запишите в обычной форме подстановок: $u = (123)(4568)$, $v = (34)(52618)$, $t = (874312)(56)$, $w = (5786)$.

Решение.

$u = (123)(4568) = \begin{pmatrix}12345678\\23156874\end{pmatrix}$, $v = (34)(52618) = \begin{pmatrix}12345678\\86432175\end{pmatrix}$,

$t = (874312)(56) = \begin{pmatrix}12345678\\28136547\end{pmatrix}$, $w = (5786) = \begin{pmatrix}12345678\\12347586\end{pmatrix}$.

Дополнительные задачи: [8], с.12, №4; [8], с.14, №6; [8], с.14, №8; [9], с.186, №1634 (остальные пункты); [10], с.85, №8.12 (остальные пункты); [8], с.16, №21; [3], с.105, №1; [10], с.85, №8.14 (остальные пункты); [10], с.85, №8.13; [10], с.86, №8.20 (остальные пункты); [8], с.28, №8; [10], с.86, №8.19; [8], с.27, №4; [3], с.82, №9; [10], с.88, №8.27; [8], с.16, №14; [8], с.16, №18; [8], с.16, №19; [10], с.87, №8.22; [10], с.87, №8.24; [4], с.44, №2.3.23; [8], с.21, №14.

§5. Изоморфизм групп

Определение 5.1. Гомоморфизмом φ группы G на (в) группу G_1 называется отображение группы G на (в) группу G_1, сохраняющее операцию, заданную на группе G.

Для мультипликативной записи операций в группах G и G_1 имеем:

$$\forall\, a, b \in G \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b), \quad \text{где } \varphi(a),\ \varphi(b) \in G_1.$$

Определение 5.2. Если гомоморфизм φ является биекцией, то φ называется изоморфизмом, а группы называются изоморфными.

Принято обозначать $G \cong G_1$.

Задачи

5.1. ([8], с.6, №15) Даны две алгебраические системы: множество N с операцией умножения и множество $M = \{0; 1\}$ также с операцией умножения. Докажите, что отображение φ, ставящее каждому натуральному числу $n \neq 1$ в соответствие число $0 \in M$, а числу $n = 1$ - число $1 \in M$, является гомоморфизмом.

Решение. По условию даны системы $(N, \cdot)$, $(M, \cdot)$ и $\varphi(n) = \begin{cases} 0, & \text{если } n \neq 1, \\ 1, & \text{если } n = 1. \end{cases}$

Проверим, что для $\forall\, n_1, n_2 \in N$ $\varphi(n_1 \cdot n_2) = \varphi(n_1) \cdot \varphi(n_2)$.

1) Пусть $n_1 \neq 1$, $n_2 \neq 1$, тогда $\varphi(n_1 \cdot n_2) = 0$, $\varphi(n_1) = 0$, $\varphi(n_2) = 0$.
   Следовательно, $\varphi(n_1 \cdot n_2) = \varphi(n_1) \cdot \varphi(n_2)$.
2) Пусть $n_1 = 1$, $n_2 \neq 1$, тогда $\varphi(n_1 \cdot n_2) = 0$, $\varphi(n_1) = 1$, $\varphi(n_2) = 0$.
   Имеет место равенство $0 = 1 \cdot 0$.
3) Пусть $n_1 = n_2 = 1$, тогда $\varphi(n_1 \cdot n_2) = \varphi(n_1) = \varphi(n_2) = 1$.
   Выполняется соотношение $1 = 1 \cdot 1$.

Отображение φ - гомоморфизм системы $(N, \cdot)$ на систему $(M, \cdot)$.

5.2. ([8], с.7, №18) Докажите, что множество R^+ с операцией сложения и множество R^- с операцией сложения являются изоморфными алгебраическими системами.

Решение. Даны системы $(R^+, +)$, $(R^-, +)$; пусть $\varphi: a \to -(a)$. Тогда

$$\varphi(a + b) = -(a + b), \quad \varphi(a) + \varphi(b) = -a + (-b) = -(a + b).$$

Значит, $\varphi(a + b) = \varphi(a) + \varphi(b)$; φ - биекция.

Следовательно, $(R^+, +) \cong (R^-, -)$.

5.3. ([8], с.7, №19) Докажите, что алгебраические системы - множество M матриц вида $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, где $x \in R$, с матричным умножением и множество R с обычным сложением - изоморфны между собой.

Решение. Пусть $\varphi: x \to \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ для систем $(R, +)$ и $(M, \cdot)$, тогда

$$\varphi(x + y) = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}, \varphi(x)\cdot\varphi(y) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}.$$

Следовательно, $\varphi(x + y) = \varphi(x)\cdot\varphi(y)$. Отображение φ - биекция.

Значит, $(R, +) \cong (M, \cdot)$.

5.4. ([8], с.7, №16) Даны две алгебраические системы: множество M вещественных матриц данного порядка n с операцией матричного умножения и множество R с операцией обычного умножения. Являются ли гомоморфизмами следующие отображения системы $(M, \cdot)$ на систему $(R, \cdot)$:

а) отображение φ_1 такое, что $\varphi_1(A) = |A|$;

б) отображение φ_2 такое, что $\varphi_2(A) = a_{11}$,

где $|A|$- определитель матрицы A из M, a_{11} - элемент первой строки и первого столбца матрицы A?

Решение. а) $\forall A, B \in M$ $\varphi_1(AB) = |AB| = |A|\cdot|B| = \varphi_1(A)\cdot\varphi_1(B)$.

Отображение φ_1 сюръективно, т.к. для $\forall r \in R$ $r = \varphi_1(C)$, где

$C = \begin{pmatrix} r\,0\ldots0 \\ 0\,1\ldots0 \\ \ldots\ldots \\ 0\,0\ldots1 \end{pmatrix}$. Следовательно, φ_1 - гомоморфизм $(M, \cdot)$ на $(R, \cdot)$.

б) Пусть $n = 2$ и $A = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}$. Тогда $C = AB = \begin{pmatrix} 5 & 3 \\ 6 & 2 \end{pmatrix}$.

$a_{11} = 1,\ b_{11} = 3,\ c_{11} = 5;\ 5 \neq 1 \cdot 3.$

Следовательно, φ_2 не является гомоморфизмом.

5.5. ([8], с.7, №20) Докажите, что всякое множество с бинарной операцией изоморфно самому себе.

Решение. Рассмотрим множество A с бинарной операцией T и тождественное отображение ε: $a \to a$, являющееся биекцией.

$$\forall\ a, b \in A \quad \varepsilon(a \mathrm{T} b) = a \mathrm{T} b = \varepsilon(a) \mathrm{T} \varepsilon(b).$$

Таким образом, ε - изоморфизм.

5.6. ([8], с.7, №21) Пусть на каждом из множеств M_1 и M_2 определена бинарная операция. Докажите, что если M_1 изоморфно M_2, то и M_2 изоморфно M_1.

Решение. (M_1, T), $(M_2, \perp)$, φ: $M_1 \to M_2$, φ - изоморфное отображение. φ - биекция; следовательно, обратное отображение φ^{-1} существует и является биективным. φ^{-1} сохраняет операцию, т.к. для

$\forall\ a_2, b_2 \in M_2\ \exists\ a_1, b_1 \in M_1$ такие, что $\varphi(a_1) = a_2$, $\varphi(b_1) = b_2$ и

$$\varphi^{-1}(a_2 \perp b_2) = \varphi^{-1}(\varphi(a_1) \perp \varphi(b_1)) = \varphi^{-1}(\varphi(a_1 \mathrm{T} b_1)) = a_1 \mathrm{T} b_1 = \varphi^{-1}(a_2) \mathrm{T} \varphi^{-1}(b_2).$$

Значит, действительно, если $(M_1, \mathrm{T}) \cong (M_2, \perp)$, то $(M_2, \perp) \cong (M_1, \mathrm{T})$.

5.7. ([8], с.7, №22) Докажите, что если на каждом из множеств M_1, M_2 и M_3 определена бинарная операция и при этом M_1 изоморфно M_2, а M_2 изоморфно M_3, то M_1 изоморфно M_3.

Решение. Рассмотрим системы (M_1, T_1), (M_2, T_2), (M_3, T_3); изоморфизмы φ: $M_1 \to M_2$ и ψ: $M_2 \to M_3$. Тогда отображение $\psi\varphi$: $M_1 \to M_3$ обладает свойствами:

1) Это отображение биективно. 2) $\psi\varphi$ сохраняет операцию T_1.

Действительно, $\forall\ a_1, b_1 \in M_1$ $\psi\varphi(a_1 \mathrm{T}_1 b_1) = \psi(\varphi(a_1 \mathrm{T}_1 b_1)) =$

$$= \psi(\varphi(a_1) \mathrm{T}_2 \varphi(b_1)) = \psi(\varphi(a_1)) \mathrm{T}_3 \psi(\varphi(b_1)) = \psi\varphi(a_1) \mathrm{T}_3 \psi\varphi(b_1).$$

Замечание 5.1. Из задач 5.5. - 5.7 следует, что отношение изоморфизма на множестве групп есть отношение эквивалентности.

5.8. ([7], с.46, №2.4.1) Пусть C - мультипликативное множество всех комплексных чисел, R - мультипликативное множество всех вещественных чисел, φ_1 - отображение C в R, согласно которому для каждого $z \in C$ $\varphi_1(z) = |z|$; φ_2 - отображение C в R, согласно которому $\varphi_2(z) = |z| + 1$; φ_3 - отображение C в R, согласно которому

$\varphi_3(z) = 0$; φ_4 - отображение C в R, согласно которому $\varphi_4(z) = 2$. Выяснить, какие из отображений φ_1, φ_2, φ_3, φ_4 являются гомоморфизмами.

Решение. Рассмотрим $(C, \cdot)$ и $(R, \cdot)$.

1) φ_1: $a \to |a|$;

$\varphi_1(ab) = |ab|$; $\varphi_1(a)\varphi_1(b) = |a|\cdot|b|$; значит, $\varphi_1(ab) = \varphi_1(a)\varphi_1(b)$.

Отображение φ_1 - гомоморфизм.

2) φ_2: $a \to |a| + 1$;

$\varphi_2(ab) = |ab| + 1$; $\varphi_2(a)\varphi_2(b) = (|a| + 1)(|b| + 1) = |ab| + |a| + |b| + 1$; значит, $|ab| + 1 \neq |ab| + |a| + |b| + 1$ при $a \neq 0$, $b \neq 0$.

Отображение φ_2 не является гомоморфизмом.

3) φ_3: $a \to 0$;

$$\varphi_3(ab) = 0; \quad \varphi_3(a)\varphi_3(b) = 0\cdot 0 = 0.$$

Следовательно, φ_3 - гомоморфизм.

4) φ_4: $a \to 2$;

$$\varphi_4(ab) = 2; \quad \varphi_4(a)\varphi_4(b) = 2\cdot 2 = 4, \quad 2 \neq 4.$$

Таким образом, φ_4 - не гомоморфизм.

5.9. ([2], с.10, №1) Даны две алгебраические системы: множество Z целых чисел с операцией умножения и конечное множество $\{-1; 0; 1\}$ также с операцией умножения. Поставим в соответствие каждому целому положительному числу число 1, каждому отрицательному числу - число -1, числу 0 - число 0. Докажите, что построенное отображение является гомоморфизмом.

Решение.

$$\varphi: a \to \begin{cases} 1, & \text{если } a > 0, \\ 0, & \text{если } a = 0, \\ -1, & \text{если } a < 0. \end{cases}$$

1) Пусть $a > 0$, $b > 0$, тогда $\varphi(ab) = 1$; $\varphi(a)\cdot\varphi(b) = 1\cdot 1 = 1$, значит,

$$\varphi(ab) = \varphi(a)\cdot\varphi(b).$$

Аналогично рассматриваются случаи: 2) $a > 0$, $b < 0$; 3) $a < 0$, $b < 0$; 4) $a = 0$, $b = 0$; 5) $a = 0$, $b > 0$; 6) $a = 0$, $b < 0$.

Из 1) - 6) следует, что φ - гомоморфизм.

5.10. ([8], с.7, №24) Докажите, что алгебраические системы - множество N с операцией сложения, множество M отрицательных

четных чисел также с операцией сложения и множество $S = \{2, 2^2, \ldots, 2^n, \ldots\}$ с операцией умножения - изоморфны между собой.

Решение.

а) Рассмотрим $(N, +)$ и $(M, +)$. Пусть φ: $n \to -2n$.

$$\varphi(n + m) = -2(n + m);\ \varphi(n) + \varphi(m) = (-2n) + (-2m) = -2(n + m),$$

значит, $\varphi(n + m) = \varphi(n) + \varphi(m)$. Отображение φ, очевидно, биекция.

Следовательно, $(N, +) \cong (M, +)$.

б) Рассмотрим $(N, +)$ и $(S, \cdot)$. Пусть ψ: $n \to 2^n$.

$$\psi(n + m) = 2^{n+m};\ \psi(n)\psi(m) = 2^n \cdot 2^m = 2^{n+m},$$

значит, $\psi(n + m) = \psi(n) + \psi(m)$; ψ - биекция.

Следовательно, $(N, +) \cong (S, \cdot)$.

в) $(M, +) \cong (S, \cdot)$ согласно замечанию 5.1.

5.11. ([8], с.7, №17) Даны три алгебраические системы: множество N с операцией сложения, множество $M_1 = \{x \mid x = 2k,\ k \in N\}$ также с операцией сложения и множество $M_2 = \{x \mid x = 2k + 1,\ k \in N\}$ с операцией умножения. Выясните, какие из этих систем изоморфны между собой.

Решение. $(N, +)$, $(M_1, +)$, $(M_2, \cdot)$.

1) Рассмотрим $(N, +)$ и $(M_1, +)$. Пусть φ: $a \to 2a$. Очевидно, φ - биекция.

$$\varphi(a + b) = 2(a + b);\ \varphi(a) + \varphi(b) = 2a + 2b = 2(a + b),$$

значит, $\varphi(a + b) = \varphi(a) + \varphi(b)$.

Следовательно, $(N, +) \cong (M_1, +)$.

2) Рассмотрим $(N, -)$ и $(M_2, \cdot)$. Пусть существует гомоморфное отображение φ: $N \to M_2$. Тогда

$$\varphi(1) = 2a + 1,\ \varphi(2) = \varphi(1 + 1) = (2a + 1)^2, \ldots, \varphi(k) = (2a + 1)^k.$$

Степенями числа $2a + 1$ не исчерпывается множество M_2. Отображение φ не является сюръективным, следовательно, получено противоречие.

Системы $(N, +)$ и $(M_2, \cdot)$ не изоморфны.

5.12. ([5], с.39, №2.2.6) Даны следующие отображения R в R:

а) $x \to x^2$,

б) $x \to 2^x$,

в) $x \to \begin{cases} \ln x^2, & \text{если } x \neq 0, \\ 0, & \text{если } x = 0, \end{cases}$

г) $x \to -x$,

д) $x \to \sin x$,

е) $x \to x$,

ж) $x \to 5x$,

з) $x \to |x|$,

и) $x \to \frac{x}{2}$,

к) $x \to 0$,

л) $x \to 1$.

Какие из этих отображений являются гомоморфными (изоморфными) отображениями групп: 1) $(R, +) \to (R, +)$, 2) $(R, +) \to (R, \cdot)$?

Решение.

1) Рассмотрим отображения $(R, +) \to (R, +)$.

а) $\varphi: x \to x^2$.

$$\varphi(a + b) = (a + b)^2,\ \varphi(a) + \varphi(b) = a^2 + b^2,\ (a + b)^2 \neq a^2 + b^2;$$

значит, отображение φ - не гомоморфизм.

б) $\varphi: x \to 2^x$.

$$\varphi(a + b) = 2^{a+b},\ \varphi(a) + \varphi(b) = 2^a + 2^b,\ 2^{a+b} \neq 2^a + 2^b;$$

отображение φ - не гомоморфизм.

в) $\varphi: x \to \begin{cases} \ln x^2, & \text{если } x \neq 0, \\ 0, & \text{если } x = 0. \end{cases}$ Пусть $a \neq 0$, $b \neq 0$ и $a + b \neq 0$, тогда

$$\varphi(a + b) = \ln(a + b)^2,$$

$$\varphi(a) + \varphi(b) = \ln a^2 + \ln b^2, \text{ но } \ln(a + b)^2 \neq \ln a^2 + \ln b^2.$$

Отображение φ не является гомоморфным.

г) $\varphi: x \to -x$.

Легко понять, что φ сохраняет сложение, является биекцией, следовательно, будет изоморфизмом.

д) $\varphi: x \to \sin x$.

Так как $\sin(a + b) \neq \sin a + \sin b$, то φ не является гомоморфизмом.

е) $\varphi: x \to x$. Очевидно, что φ - изоморфизм.

ж) $\varphi: x \to 5x$.

$$\varphi(a + b) = 5(a + b),\ \varphi(a) + \varphi(b) = 5a + 5b = 5(a + b),$$

значит, отображение φ является гомоморфным.

$$\forall\, a, b \in R\ \ a \neq b \Rightarrow \varphi(a) \neq \varphi(b),$$ т.е. φ инъективно.

Кроме того, отображение φ сюръективно; следовательно, φ является изоморфизмом.

з) $\varphi: x \to |x|$.

$|a + b| \neq |a| + |b|$. Отображение φ не является гомоморфизмом.

и) $\varphi: x \to \frac{x}{2}$.

$$\varphi(a + b) = \frac{a+b}{2} = \frac{a}{2} + \frac{b}{2} = \varphi(a) + \varphi(b).$$

$$\forall\, a, b \in R\ \ a \neq b \Rightarrow \varphi(a) \neq \varphi(b),$$ значит, φ инъективно.

Кроме того, φ сюръективно. Следовательно, φ - изоморфизм.

к) $\varphi: x \to 0$.

$\varphi(a + b) = 0 = 0 + 0 = \varphi(a) + \varphi(b)$, т.е. φ сохраняет операцию.

$\forall\ a, b \in R\quad \varphi(a) = \varphi(b)$; следовательно, отображение φ не изоморфно.

л) $\varphi: x \to 1$.

$$\varphi(a + b) = 1,\ \varphi(a) + \varphi(b) = 1 + 1 = 2,\ 1 \neq 2.$$

Отображение φ не является гомоморфизмом.

2) Рассмотрим отображения $(R, +) \to (R, \cdot)$.

а) $\varphi: x \to x^2$.

$$\varphi(a + b) = (a + b)^2,\ \varphi(a)\cdot\varphi(b) = a^2b^2,\ \varphi(a + b) \neq \varphi(a)\cdot\varphi(b).$$

Отображение φ - не гомоморфизм.

б) $\varphi: x \to 2^x$.

$$\varphi(a + b) = 2^{a+b},\quad \varphi(a)\cdot\varphi(b) = 2^a\cdot 2^b = 2^{a+b}.$$

Отображение φ является гомоморфизмом. Но отображение не сюръективно, т.к. $\forall\ x \in R\quad 2^x > 0$.

Следовательно, φ - не изоморфизм.

в) $\varphi: x \to \begin{cases} \ln x^2, & \text{если } x \neq 0, \\ 0, & \text{если } x = 0. \end{cases}$

$\ln(a + b)^2 \neq \ln a^2 \cdot \ln b^2$, здесь $a \neq 0$, $b \neq 0$ и $a + b \neq 0$.

Отображение φ - не гомоморфизм.

г) $\varphi: x \to -x$.

$-(a + b) \neq (-a)(-b)$. Отображение φ не является гомоморфизмом.

д) $\varphi: x \to \sin x$.

$\sin(a + b) \neq \sin a \cdot \sin b$. Отображение φ - не гомоморфизм.

е) $\varphi: x \to x$.

$a + b \neq a\cdot b$. Отображение не сохраняет операцию.

ж) $\varphi: x \to 5x$.

$5(a + b) \neq 5a\cdot 5b$.

Отображение не является гомоморфизмом.

з) $\varphi: x \to |x|$.

$|a + b| \neq |a|\cdot|b|$.

Отображение φ не гомоморфно.

и) $\varphi: x \to \frac{x}{2}$.

$\frac{a+b}{2} \neq \frac{a}{2}\cdot\frac{b}{2}$. Отображение не является гомоморфным.

к) $\varphi: x \to 0$.

$0 = 0\cdot 0$. Отображение φ гомоморфно, но поскольку оно не инъективно, изоморфным не является.

л) φ: $x \to 1$.

$1 = 1 \cdot 1$. Отображение - гомоморфизм.

$\forall\ a, b \in R \quad \varphi(a) = \varphi(b)$, следовательно, φ - не изоморфизм.

5.13. ([5], с.40, №2.2.10) Докажите, что следующие группы не изоморфны: а) $(Z, +)$ и $(N, +)$, б) $(Z, \cdot)$ и $(2Z, \cdot)$, в) $(M(2,R), \cdot)$ и $(R, \cdot)$, где $M(2,R)$ - множество квадратных матриц второго порядка с действительными элементами.

Решение.

а) $(Z, +)$ и $(N, +)$.

Пусть существует изоморфизм φ. Тогда $\varphi(0) = n$, где $n \in N$.

$n = \varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0) = n + n$. Но в N равенство $n = n + n$ не выполняется. Следовательно, не существует изоморфного отображения φ.

Системы не изоморфны.

б) $(Z, \cdot)$ и $(2Z, \cdot)$.

Предположим, что существует изоморфизм φ. Тогда $\varphi(1) = 2n$, где $n \in Z$, $\varphi(2) = 2l$, где $l \in Z$; $2l = \varphi(2) = \varphi(2 \cdot 1) = \varphi(2) \cdot \varphi(1) = 2l \cdot 2n$. Последнее возможно при $l = 0$ или $n = 1$.

Сначала рассмотрим случай $l = 0$. Тогда $\varphi(2) = 0$ и $\varphi(4) = \varphi(2 \cdot 2) = 0 \cdot 0 = 0$, что противоречит инъективности φ.

Пусть теперь $n = 1$. Тогда $\varphi(1) = 2$ и $2 = \varphi((-1)^2) = (\varphi(-1))^2$, что невозможно, т.к. $\varphi(-1) \in 2Z$.

Значит, алгебраические системы $(Z, \cdot)$ и $(2Z, \cdot)$ не изоморфны.

в) $(M(2,R), \cdot)$ и $(R, \cdot)$.

1) Пусть существует изоморфное отображение φ. Тогда $\varphi(M(2,R)) = R$, т.к. φ - сюръекция.

Покажем, что $\varphi(O) = 0$, где $O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Действительно,

$$\forall\ A \in M(2,R)\ \ A \cdot O = O,\ \varphi(A \cdot O) = \varphi(A)\varphi(O) = \varphi(O).$$

Последнее равенство выполняется для любого действительного числа $\varphi(A)$, что возможно только при $\varphi(O) = 0$.

2) Очевидно, что $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. (*)

φ - инъекция, следовательно, из $\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} \neq \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$ и $\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix} \neq \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$

должно следовать, что $\varphi\left(\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\right) \neq 0$ и $\varphi\left(\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\right) \neq 0$. Но тогда из (*)

имеем $\varphi\left(\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\right)\varphi\left(\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\right) = 0$, что невозможно.

Алгебраические системы $(M(2,R), \cdot)$, $(R, \cdot)$ не изоморфны.

5.14. ([5], с.49, №2.3.60) Существует ли гомоморфное отображение φ аддитивной группы целых чисел в себя, при котором:
а) $\varphi(2) = 3$; б) $\varphi(2) = 4$?

Решение.

а) Пусть φ - гомоморфизм и $\varphi(1) = a$, где $a \in Z$. Тогда

$$\varphi(2) = \varphi(1 + 1) = \varphi(1) + \varphi(1) = a + a.$$

По условию $\varphi(2) = 3$. Но в Z равенство $3 = 2a$ не выполняется. Следовательно, не существует гомоморфного отображения φ, при котором $\varphi(2) = 3$.

б) Зададим отображение φ: $m \to 2m$, где $m \in Z$.

φ - гомоморфизм, при котором $\varphi(2) = 4$.

5.15. ([8], с.28, №9) Докажите, что группа

$$F = \left\{ f_0 = x,\ f_1 = \frac{1}{x},\ f_2 = 1 - x,\ f_3 = \frac{x}{x-1},\ f_4 = \frac{x-1}{x},\ f_5 = \frac{1}{1-x} \right\}$$

изоморфна симметрической группе S_3 третьей степени.

Решение. Воспользуемся таблицами Кэли для групп S_3 и F. Таблица Кэли группы S_3 помещена на с.27. Построение таблицы умножения для группы F выполнено при решении задачи №8 из [8, с.28] (см. список дополнительных задач §4). Она имеет следующий вид:

·	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_0	f_5	f_4	f_3	f_2
f_2	f_2	f_4	f_0	f_5	f_1	f_3
f_3	f_3	f_5	f_4	f_0	f_2	f_1
f_4	f_4	f_2	f_3	f_1	f_5	f_0
f_5	f_5	f_3	f_1	f_2	f_0	f_4

Если в таблице для группы F заменить элементы f_0, f_1, f_2, f_3, f_4, f_5 соответственно элементами p_0, p_3, p_4, p_5, p_2, p_1 группы S_3, то получим таблицу Кэли для группы S_3

$$\varphi: f_0 \to p_0,\ f_1 \to p_3,\ f_2 \to p_4,\ f_3 \to p_5,\ f_4 \to p_2,\ f_5 \to p_1.$$

Следовательно, φ - изоморфизм.

5.16. ([3], с.93, №18) Показать, что мультипликативная группа M корней четвертой степени из единицы и группа A с операцией, заданной таблицей 2, изоморфны.

Решение. $M = \{1, -1, i, -i\}$, $A = \{b_0, b_1, b_2, b_3\}$.

1

·	**1**	**-1**	***i***	***-i***
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
-i	$-i$	i	1	-1

2

·	$\boldsymbol{b_0}$	$\boldsymbol{b_1}$	$\boldsymbol{b_2}$	$\boldsymbol{b_3}$
$\boldsymbol{b_0}$	b_0	b_1	b_2	b_3
$\boldsymbol{b_1}$	b_1	b_2	b_3	b_0
$\boldsymbol{b_2}$	b_2	b_3	b_0	b_1
$\boldsymbol{b_3}$	b_3	b_0	b_1	b_2

Обе группы содержат одно и то же количество элементов. Следовательно, между ними можно установить взаимно однозначное соответствие. Нам нужно установить такое соответствие, которое не нарушалось бы при умножении.

1) Известно, что при изоморфизме групп единичный элемент одной группы соответствует единичному элементу другой, поэтому $1 \leftrightarrow b_0$.

2) Так как соответствие должно сохраняться при умножении и

$$(-1)^2 = 1, \text{ а } b_1^2 = b_2 \neq b_0 \text{ и } b_3^2 = b_2 \neq b_0,$$

то числу -1 не может соответствовать ни элемент b_1, ни элемент b_3.

Значит, $-1 \leftrightarrow b_2$ (действительно, $b_2^2 = b_0$).

3) Оставшиеся две пары элементов сопоставим следующим образом:

$$i \leftrightarrow b_1, \quad -i \leftrightarrow b_3.$$

Таким образом, имеем взаимно однозначное соответствие:

$$1 \leftrightarrow b_0, \quad i \leftrightarrow b_1, \quad -1 \leftrightarrow b_2, \quad -i \leftrightarrow b_3.$$

4) Покажем, что это соответствие сохраняется при умножении. Составим таблицу для M, записав в заглавные строку и столбец элементы 1, -1, i, $-i$ в том порядке, в каком записаны в таблице группы A соответствующие им элементы b_i. Тогда таблица умножения имеет вид.

3

·	**1**	***i***	**-1**	***-i***
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
-i	$-i$	1	i	-1

Теперь посмотрим, находятся ли в одинаковых клетках таблиц 2 и 3 соответствующие элементы. В обведенных клетках находятся соответствующие элементы i и b_1. Аналогично и для других пар элементов. Если обозначить $b_0 = 1$, $b_1 = i$, $b_2 = -1$, $b_3 = -i$, то группа A ничем не будет отличаться от группы M.

Следовательно, группы M и A изоморфны.

Дополнительные задачи: [7], с.46, №2.4.3; [9], с.188, №1640; [5], с.39, №2.2.5; [5], с.39, №2.2.6 (остальные пункты); [5], с.40,№2.2.7; [5], с.40, №2.2.8; [5], с.47, №2.3.49; [3], с.95, №19.

§6. Подгруппы

Определение 6.1. Пусть $G_1 \subseteq G$, G - группа. Непустое множество G_1 называется подгруппой группы G, если оно является группой относительно заданной на нем операции.

Теорема 6.1. (критерий подгруппы) Для того, чтобы непустое подмножество G_1 группы G с операцией T было подгруппой, необходимо и достаточно выполнения двух условий:

1°. для любых элементов $a, b \in G_1$ выполняется $a \mathrm{T} b \in G_1$;

2°. для любого элемента $a \in G_1$ обратный ему элемент $a' \in G_1$.

Условия 1° и 2° можно заменить следующим одним условием:

3°. для любых двух элементов $a, b \in G_1$ элемент $a \mathrm{T} b' \in G_1$.

Задачи

6.1. ([8], с.21, №5) Докажите, что множество четных чисел является подгруппой аддитивной группы Z целых чисел. Является ли множество нечетных чисел подгруппой группы Z?

Решение. а) Множество четных чисел обозначим

$$A = \{ n \mid n = 2k, k \in Z\}, A \subset Z.$$

1) $\forall\, n_1, n_2 \in A \;\; n_1 = 2k_1, \;\; n_2 = 2k_2, n_1 + n_2 = 2k_1 + 2k_2 = 2(k_1 + k_2) \in A$, значит, выполняется условие 1° критерия подгруппы.

2) $\forall\, n \in A \;\; n = 2k \quad -n = -2k = 2(-k) \in A$, значит, выполняется условие 2° критерия подгруппы.

Следовательно, A - подгруппа группы Z.

б) Множество нечетных чисел обозначим

$$A_1 = \{ n \mid n = 2k + 1, k \in Z\}, A_1 \subset Z.$$

1) $\forall\, n_1, n_2 \in A_1 \;\; n_1 = 2k_1 + 1, n_2 = 2k_2 + 1.$

$$n_1 + n_2 = (2k_1 + 1) + (2k_2 + 1) = 2(k_1 + k_2 + 1) \notin A_1,$$

т.е. условие 1° критерия подгруппы не имеет места.

A_1 - не подгруппа группы Z.

6.2. ([9], с.189, №1649) Какие из подгрупп задачи №1634 ([9],с.186)

являются подгруппами других из этих групп?

Решение.

1) Рассмотрим группы $(Q^+, \cdot)$ и $(Q\backslash\{0\}, \cdot)$.

а) $\forall\, a, b \in Q^+ \;\; ab \in Q^+$, условие 1^o выполняется.

б) $\forall\, a \in Q^+ \;\; a^{-1} \in Q^+$, условие 2^o имеет место.

$(Q^+, \cdot)$ является подгруппой группы $(Q\backslash\{0\}, \cdot)$.

2) Рассмотрим группы $M = \{A \mid A \in Z^{n\times n}, |A| = 1\}$ и

$M_1 = \{A \mid A \in R^{n\times n}, |A| \neq 0\}$ с операцией умножения.

а) $\forall\, A, B \in M \;\; AB \in M$, т.к. $AB \in Z^{n\times n}$ и $|AB| = |A|\cdot|B| = 1$.

б) $\forall\, A \in M \;\; A^{-1} \in Z^{n\times n}$ и $|A^{-1}| = 1$.

Оба условия критерия подгруппы выполняются. Следовательно, M является подгруппой M_1.

6.3. ([5], с.46, №2.3.36) Какие из следующих множеств подстановок образуют подгруппу в группе S_4:

а) $\left\{\begin{pmatrix}1234\\1234\end{pmatrix}, \begin{pmatrix}1234\\4312\end{pmatrix}, \begin{pmatrix}1234\\2143\end{pmatrix}, \begin{pmatrix}1234\\3421\end{pmatrix}\right\}$; в) $\left\{\begin{pmatrix}1234\\1234\end{pmatrix}, \begin{pmatrix}1234\\4312\end{pmatrix}, \begin{pmatrix}1234\\1243\end{pmatrix}, \begin{pmatrix}1234\\4321\end{pmatrix}\right\}$?

Решение. а) Пусть $e = \begin{pmatrix}1234\\1234\end{pmatrix}$, $a = \begin{pmatrix}1234\\4312\end{pmatrix}$, $b = \begin{pmatrix}1234\\2143\end{pmatrix}$, $c = \begin{pmatrix}1234\\3421\end{pmatrix}$.

Найдем попарные произведения: $aa = b$, $ab = c$, $ac = e$, $ba = c$, $bb = e$, $bc = a$, $ca = e$, $cb = a$, $cc = b$.

Множество замкнуто относительно операции и взятия обратного элемента.

Следовательно, оно является подгруппой группы S_4.

в) Пусть $e = \begin{pmatrix}1234\\1234\end{pmatrix}$, $a = \begin{pmatrix}1234\\4312\end{pmatrix}$, $b = \begin{pmatrix}1234\\1243\end{pmatrix}$, $c = \begin{pmatrix}1234\\4321\end{pmatrix}$.

Найдем попарные произведения элементов этого множества.

$$aa = \begin{pmatrix}1234\\4312\end{pmatrix}\begin{pmatrix}1234\\4312\end{pmatrix} = \begin{pmatrix}1234\\2143\end{pmatrix},$$

aa не является элементом множества, значит, оно не будет подгруппой группы S_4.

В §4 были рассмотрены группы подстановок. Всякая такая группа конечна и имеет порядок $n!$, где n - степень подстановки. Важность этих групп определяется тем, что их подгруппами в известном смысле исчерпываются все конечные группы. Именно, справедлива следующая теорема.

Теорема 6.2. (теорема Кэли) Любая конечная группа G порядка n изоморфна некоторой подгруппе G' симметрической группы S_n подстановок n-ой степени.

6.4. ([8], с.28, №10) На множестве $G = \{c_1, c_2, c_3, c_4\}$ задана таблицей Кэли некоторая операция:

$\cdot$	c_1	c_2	c_3	c_4
c_1	c_3	c_4	c_1	c_2
c_2	c_4	c_3	c_2	c_1
c_3	c_1	c_2	c_3	c_4
c_4	c_2	c_1	c_4	c_3

Докажите, что G - группа относительно заданной операции; укажите подгруппу симметрической группы S_4 четвертой степени, которой изоморфна группа G; изоморфно отобразите группу G на группу самосовмещений ромба.

Решение.

1) Операция обратима, т.к. в каждом столбце и каждой строке таблицы имеются все элементы множества G.

2) Для проверки ассоциативности воспользуемся теоремой Кэли. Таблица показывает, что после умножения элемента c_1 слева на элементы c_1, c_2, c_3, c_4 получаются элементы c_3, c_4, c_1, c_2.

По индексам элементов c_1, c_2, c_3, c_4 и c_3, c_4, c_1, c_2 элементу c_1 поставим в соответствие подстановку $p_1 = \begin{pmatrix} 1234 \\ 3412 \end{pmatrix}$. Аналогично

$$c_2 \to p_2 = \begin{pmatrix} 1234 \\ 4321 \end{pmatrix}, \; c_3 \to p_3 = \begin{pmatrix} 1234 \\ 1234 \end{pmatrix}, \; c_4 \to p_4 = \begin{pmatrix} 1234 \\ 2143 \end{pmatrix}.$$

Пусть $G_1 = \{p_1, p_2, p_3, p_4\}$. Для множества G_1 построим таблицу Кэли. Она будет совпадать с таблицей умножения множества G, если в последней выполнить переобозначение элементов: $c_i \leftrightarrow p_i$, $i = 1, 2, 3, 4$. По таблице умножения для G_1 определяем, что операция, заданная на G_1, обратима. Кроме того, умножение подстановок, как частный случай умножения преобразований, ассоциативно. Следовательно, G_1 - группа. Множество G, очевидно, изоморфно группе G_1. Таким образом, G также является группой. Отсюда следует ассоциативность операции, заданной на G. Заметим, что можно было не устанавливать обратимость операции в G. Последнее также следует из того, что G - группа.

3) Пусть $M = \{e, a, b, c\}$- группа самосовмещений ромба. Воспользуемся таблицей Кэли из задачи 4.18. Ясно, что соответствие φ: $c_3 \to e$, $c_1 \to a$, $c_2 \to b$, $c_4 \to c$ является изоморфизмом группы G на группу M.

6.5. ([8], с.29, №12) Элементы группы M самосовмещений квадрата представьте подстановками четвертой степени. Составьте для

группы M таблицу Кэли. Изоморфно отобразите группу M на одну из подгрупп симметрической группы S_8 восьмой степени.

Решение.

1) Воспользуемся задачей 4.20, при решении которой найдено представление элементов группы M подстановками из S_4 и составлена таблица Кэли (с.31).

2) По индексам элементов $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7$ и индексам полученных элементов $a_1, a_2, a_3, a_0, a_5, a_6, a_7, a_4$ элементу a_1 поставим в соответствие подстановку $g_1 = \begin{pmatrix} 12345678 \\ 23416785 \end{pmatrix}$. Аналогично сопоставим элементам $a_0, a_2, a_3, a_4, a_5, a_6, a_7$ подстановки из S_8

$g_0 = \begin{pmatrix} 12345678 \\ 12345678 \end{pmatrix}$, $g_2 = \begin{pmatrix} 12345678 \\ 34127856 \end{pmatrix}$, $g_3 = \begin{pmatrix} 12345678 \\ 41238567 \end{pmatrix}$, $g_4 = \begin{pmatrix} 12345678 \\ 58761432 \end{pmatrix}$,

$g_5 = \begin{pmatrix} 12345678 \\ 65872143 \end{pmatrix}$, $g_6 = \begin{pmatrix} 12345678 \\ 76583214 \end{pmatrix}$, $g_7 = \begin{pmatrix} 12345678 \\ 87654321 \end{pmatrix}$ соответственно.

Подстановки $g_0, g_1, \ldots, g_7$ образуют искомую подгруппу.

Дополнительные задачи: [8], с.21, №6; [9], с.189, №1649 (остальные пункты); [8], с.25, №2; [5], с.46, №2.3.36.

§7. Порядок элемента группы. Циклические группы

Определение 7.1. Число элементов конечной группы называется порядком группы.

Определение 7.2. Пусть G - группа, $g \in G$, n - натуральное число, большее единицы. Произведение n элементов, равных элементу g, называется n-ой степенью элемента g и обозначатся g^n.

Полагаем $g^1 = g$.

Далее, условимся считать нулевой степенью элемента g единичный элемент этой группы, т.е. $g^0 = e$.

Определение 7.3. Пусть n - натуральное число. Тогда полагаем $g^{-n} = (g^{-1})^n$.

Элементы $g^{-2}, g^{-3}, \ldots$ являются, как легко проверить, обратными соответственно для элементов $g^2, g^3, \ldots$.

Определение 7.4. Порядком элемента g называется наименьший натуральный показатель степени такой, что $g^n = e$. Если для любого числа n из N $g^n \neq e$, то элемент g называется элементом бесконечного порядка.

Порядок элемента обозначается $O(g)$. В случае элемента бесконечного порядка пишут, что $O(g) = \infty$.

Пусть G - произвольная группа и g - некоторый её элемент. Рассмотрим множество G', состоящее из целых степеней элемента g:

$$G' = \{\dots, g^{-2}, g^{-1}, g^0, g^1, g^2, \dots\}.$$

Совокупность всех степеней элемента g образует, очевидно, коммутативную подгруппу группы G.

Определение 7.5. Группа G называется циклической группой, если она состоит из степеней одного из своих элементов g, то есть совпадает с одной из своих циклических подгрупп.

Элемент g называется образующим (порождающим) элементом циклической группы G. Обозначение: $G = (g)$.

Теорема 7.1. Всякая подгруппа циклической группы сама является циклической группой.

Задачи

7.1. ([8], с.21, №8) Докажите, что множество целых степеней числа 3 является подгруппой мультипликативной группы $Q\backslash\{0\}$. Запишите эту подгруппу символически. Является ли она циклической? Каков порядок элемента, порождающего эту подгруппу?

Решение. Пусть $A = \{a \mid a = 3^n, n \in Z\}$, $A \subset Q\backslash\{0\}$.

1) $\forall\ a, b \in A\ \ a = 3^n, b = 3^m,\ \ ab = 3^n \cdot 3^m = 3^{n+m} \in A$, значит, множество A замкнуто относительно умножения.

2) $\forall\ \ a = 3^n\ \ a^{-1} = 3^{-n} \in A$, т.е. множество A замкнуто относительно взятия обратного элемента. Множество A является подгруппой мультипликативной группы $Q\backslash\{0\}$. A - циклическая подгруппа, т.к. состоит из целых степеней элемента 3, т.е. $A = (3)$. Число 3 является элементом бесконечного порядка.

7.2. ([5], с.152, №8.2.27) Для каждой из следующих групп определите, является ли она циклической:

а) $(Z, +)$; б) $(Q, +)$; в) $(Q\backslash\{0\}, \cdot)$; г) $(6Z, +)$; д) $(\{6^n \mid n \in Z\}, \cdot)$;

е) $(\{a + b\sqrt{2} \mid a, b \in Z\}, +)$; ж) $(Z_4, +)$; з) $(Z_7^*, \cdot)$; и) $(Z_8^*, \cdot)$; к) $(Z_9^*, \cdot)$.

Решение.

а) Да, т.к. образующим элементом данной группы является число 1: $Z = (1)$. Число -1 - также образующий элемент и других образующих элементов в группе нет (подумайте, почему).

б) Нет, т.к. если предположить, что у группы $(Q, +)$ есть образующий элемент g, то его кратные должны образовывать множество Z как подгруппу

группы Q. Значит, $g = 1$ или $g = -1$. Но тогда $(g) = Z$, а $Z \neq Q$.

в) Нет, т.к. множество элементов циклической группы счетное, а множество $Q \setminus \{0\}$ не является счетным. (Можно рассуждать так же, как в б)).

г) Да, т.к., например, 6 - образующий элемент: $_6Z = (6)$.

д) Да, т.к. $\{6^n | \ n \in Z\} = \{..., 6^{-3}, 6^{-2}, 6^{-1}, 6^0, 6^1, 6^2, 6^3, ...\}$.

е) Нет. Решение аналогично б).

ж) Да, т.к. $\bar{1}$ - образующий элемент: $Z_4 = (\bar{1})$.

з) Да, т.к. в группе существует элемент шестого порядка. Таким является, например, элемент $\bar{3}$. Действительно, $\bar{3}^2 = \bar{9} = \bar{2}$, $\bar{3}^3 = \bar{2} \cdot \bar{3} = \bar{6}$,

$$\bar{3}^4 = \bar{6} \cdot \bar{3} = \bar{4}, \quad \bar{3}^5 = \bar{4} \cdot \bar{3} = \bar{5}, \quad \bar{3}^6 = \bar{5} \cdot \bar{3} = \bar{1}.$$

и) Нет, т.к. порядки всех элементов группы меньше 7. Действительно,

$$Z_8^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \quad \text{и} \quad \bar{3}^2 = \bar{1}, \quad \bar{5}^2 = \bar{1}, \quad \bar{7}^2 = \bar{1}.$$

к) Да, т.к. элемент $\bar{2}$ из Z_9^* имеет порядок, равный 6, и

$$Z_9^* = \{\bar{2}^1, \bar{2}^2, \bar{2}^3, \bar{2}^4, \bar{2}^5, \bar{2}^6\}.$$

7.3. ([5], с.149, №8.2.6) В мультипликативной группе комплексных чисел C^* найдите все элементы порядка 2, 4, 6.

Решение.

1) Если элемент x из C^* имеет порядок 2, то $x^2 = 1$. Значит, x является корнем второй степени из 1. В группе $\sqrt{1} = \{1; -1\}$ $O(1) = 1$; $(-1)^2 = 1$, поэтому $O(-1) = 2$. Искомый элемент $x = -1$.

2) Рассмотрим подгруппу $\sqrt[4]{1} = \{1, -1, i, -i\}$ в C^*. Порядки 1, -1 известны. Найдем порядки элементов i и $-i$: $i^2 = -1$, $i^3 = -i$, $i^4 = 1$. Тогда $O(i) = 4$. Аналогично находим, что $O(-i) = 4$. Искомые элементы порядка 4 в группе C^* - числа i и i.

3) Рассмотрим в группе C^* подгруппу

$$\sqrt[6]{1} = \{1, \frac{1}{2} + i\frac{\sqrt{3}}{2}, \frac{1}{2} - i\frac{\sqrt{3}}{2}, -1, -\frac{1}{2} - i\frac{\sqrt{3}}{2}, -\frac{1}{2} + i\frac{\sqrt{3}}{2}\}.$$

Для нахождения порядков элементов удобно использовать тригонометрическую форму записи комплексных чисел. Например,

$$\frac{1}{2} + i\frac{\sqrt{3}}{2} = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3}.$$

Применяя формулу Муавра, найдем, что $O(\frac{1}{2} + i\frac{\sqrt{3}}{2}) = 6$; $O(\frac{1}{2} - i\frac{\sqrt{3}}{2}) = 3$; $O(-\frac{1}{2} - i\frac{\sqrt{3}}{2}) = 3$; $O(-\frac{1}{2} + i\frac{\sqrt{3}}{2}) = 6$. Порядок 6 имеют два элемента: $\frac{1}{2} + i\frac{\sqrt{3}}{2}$ и $-\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

Другое решение этой задачи можно получить с помощью геометрических представлений (см. задачу 7.8).

7.4. ([8], с.21, №12) Найдите порядки всех элементов:
а) в группе самосовмещений ромба;
б) в группе самосовмещений правильного треугольника.
Являются ли эти группы циклическими?

Решение.

а) Из таблицы Кэли группа самосовмещений ромба (см. задачу 4.18) следует, что $O(a) = O(b) = O(c) = 2$. Порядок единичного элемента равен 1. Группа не является циклической, т.к. порядок группы M равен четырем, а в ней нет элемента четвертого порядка.

б) Воспользуемся задачей 4.16, при решении которой была составлена таблица Кэли группы самосовмещений правильного треугольника. По таблице находим порядки элементов:

$$O(p_0) = 1,\ O(p_1) = O(p_2) = 3,\ O(p_3) = O(p_4) = O(p_5) = 2.$$

Группа не является циклической, т.к. в ней нет элемента шестого порядка.

7.5. ([8], с.21, №9) Найдите порядки элементов

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

мультипликативной группы невырожденных матриц второго порядка.

Решение. Введем обозначения: $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

1) $O(A) = 2$, т.к. $A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

2) $O(B) = \infty$, т.к. $\forall\, n \in N\ \ B^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. Докажем это индукцией по n.

Если $n = 2$, то $B^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$.

Пусть для $k \in N\ \ B^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, тогда $B^{k+1} = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix}$.

Таким образом, равенство $B^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ верно для любого натурального n.

3) $O(C) = 4$. Проверим это утверждение: $C^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$;

$$C^3 = C^2C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix};\ C^4 = (C^2)^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

7.6. ([8], с.22, №17) Найдите порядок элемента $a = (1\ 2\ 4\ 3) \in S_4$ и постройте циклическую подгруппу группы S_4, порожденную элементом a.

Решение. $a = (1\ 2\ 4\ 3) = \begin{pmatrix} 1234 \\ 2413 \end{pmatrix}$. $a^0 = e$, $a^1 = a$,

$$a^2 = \begin{pmatrix} 1234 \\ 2413 \end{pmatrix}\begin{pmatrix} 1234 \\ 2413 \end{pmatrix} = \begin{pmatrix} 1234 \\ 4321 \end{pmatrix},\ a^3 = \begin{pmatrix} 1234 \\ 4321 \end{pmatrix}\begin{pmatrix} 1234 \\ 2413 \end{pmatrix} = \begin{pmatrix} 1234 \\ 3142 \end{pmatrix},\ a^4 = e.$$

Значит, $O(a) = 4$ и

$$(a) = \{e, a, a^2, a^3\} = \left\{ \begin{pmatrix} 1234 \\ 1234 \end{pmatrix}, \begin{pmatrix} 1234 \\ 2413 \end{pmatrix}, \begin{pmatrix} 1234 \\ 4321 \end{pmatrix}, \begin{pmatrix} 1234 \\ 3142 \end{pmatrix} \right\}.$$

7.7. ([8], с.22, №19) Найдите пересечение подгрупп A и B аддитивной группы Z, если: а) $A = (2)$, $B = (3)$; б) $A = (6)$, $B = (8)$.

Решение.

а) $A \cap B = (2) \cap (3) = (6)$, т.к. общие элементы A и B делятся на 2 и на 3.

б) $A \cap B = (6) \cap (8) = (24)$, т.к. общие элементы A и B делятся на 24.

7.8. ([8], с.22, №30) В группе всех поворотов плоскости вокруг некоторой точки этой плоскости установите:

а) порядки элементов a_1, a_2, a_3, a_4, представляющих собой повороты соответственно на углы π, $2\pi/3$, $\pi/6$, $3\pi/2$ радиан;

б) поворот на какой угол дает элемент порядка 20;

в) повороты на какие углы являются элементами конечного порядка.

Решение. а) $O(a_1) = 2$, т.к. $2 \cdot \pi = 2\pi$.

$3 \cdot (2\pi/3) = 2\pi$, следовательно, $O(a_2) = 3$;

$12 \cdot (\pi/6) = 2\pi$, следовательно, $O(a_3) = 12$;

$2 \cdot (3\pi/2) = 3\pi$, $3 \cdot (3\pi/2) = 9\pi/2$, $4 \cdot (3\pi/2) = 6\pi$, следовательно, $O(a_4) = 4$.

б) Пусть $O(x) = 20$. Тогда $20x = 2\pi$, откуда $x = \pi/10$.

в) Элементами конечного порядка являются повороты на углы вида $\frac{m}{n}\pi$, где $m, n \in Z$, $n \neq 0$.

7.9. ([5], с.149, №8.2.1) Найдите порядки элементов:

б) $\begin{pmatrix} \bar{1} & \bar{2} \\ \bar{0} & \bar{1} \end{pmatrix}$ в группе $GL(2,Z_3)$, где $GL(2,Z_3)$ - множество невырожденных матриц порядка 2 над Z_3;

г) $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ в группе $GL(2,C)$, где $GL(2,C)$ - множество невырожденных матриц порядка 2 над C.

Решение.

б) $\begin{pmatrix} \bar{1} & \bar{2} \\ \bar{0} & \bar{1} \end{pmatrix}\begin{pmatrix} \bar{1} & \bar{2} \\ \bar{0} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}$, $\begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}\begin{pmatrix} \bar{1} & \bar{2} \\ \bar{0} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}$, значит, $O\left(\begin{pmatrix} \bar{1} & \bar{2} \\ \bar{0} & \bar{1} \end{pmatrix}\right) = 3$.

г) $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$,

$\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, следовательно, $O\left(\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\right) = 4$.

7.10. ([5], с.149, №8.2.8) Проверьте, что в группе $SL(2,R)$ элементы $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ и $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ имеют порядки 4 и 3 соответственно. Покажите, что AB - элемент бесконечного порядка. Может ли в абелевой группе произведение элементов конечного порядка быть элементом бесконечного порядка?

Решение. $SL(2,R)$ - множество всех матриц второго порядка с действительными элементами, причем определитель матриц равен единице.

1) $O(A) = 4$ (см. решение задачи 7.5 3)). $O(B) = 3$, т.к.

$B^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$, $B^3 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

2) $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. В задаче 7.5 было показано, что такая матрица имеет бесконечный порядок.

3) В абелевой группе произведение элементов конечного порядка не может быть элементом бесконечного порядка, т.к. если $O(a) = n$, $O(b) = m$, то $(ab)^{nm} = (a^n)^m \cdot (b^m)^n = e$. Следовательно, $O(ab) \le O(a) \cdot O(b)$.

7.11. ([8], с.23, №32) Докажите, что множество, состоящее из матриц $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $a = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $c = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, является под-

группой мультипликативной группы невырожденных матриц второго порядка. Является ли эта группа абелевой? Является ли она циклической? Каковы её образующие элементы?

Решение. $A = \{e, a, b, c\}$. Составим таблицу умножения для A.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

1) Множество A замкнуто относительно умножения.

2) Множество A замкнуто относительно взятия обратного элемента:

$$a^{-1} = a,\ b^{-1} = c,\ c^{-1} = b,\ e^{-1} = e.$$

Следовательно, $(A, \cdot)$ является подгруппой мультипликативной группы невырожденных матриц второго порядка.

3) Подгруппа является абелевой, т.к. таблица умножения симметрична относительно главной диагонали.

4) Подгруппа является циклической, т.к. $b^0 = e,\ b^1 = b,\ b^2 = a,\ b^3 = c$. Таким образом, $A = (b)$. Элемент c также является образующим. Действительно, $c^2 = a,\ c^3 = b$. Так как $O(a) = 2$, то a образующим элементом не является.

7.12. ([8], с.23, №33) Докажите, что все подгруппы в любой циклической группе G порядка n имеют вид $\{e, a^d, a^{2d}, \ldots, a^{\frac{n}{d}-1}\}$, где d - любой натуральный делитель числа n, a - образующий элемент группы G.

Решение. 1) Рассмотрим группу $G = (a)$, пусть H - подгруппа группы G. Тогда $H = (a^r)$, где r - наименьший из натуральных s, для которых $a^s \in H$ (см. доказательство теоремы 7.1).

2) Докажем, что r делит n. Разделим n на r: $n = rq + r_1,\ 0 \le r_1 < r$.

Пусть $r_1 \neq 0$, тогда $a^{r_1} = a^{n - rq} = a^n \cdot a^{-rq} = e(a^r)^{-q} \in H$, что противоречит выбору r. Следовательно, $r_1 = 0$ и r - делитель n. Полагая $d = r$, имеем

$$H = \{e, a^d, a^{2d}, \ldots, a^{n_1 d - 1}\},$$

где n_1 найдем из условия $n = dn_1$; получаем, что $n_1 = \frac{n}{d}$.

7.13. ([8], с.23, №34) Сколько подгрупп имеет группа

$A = \{e, a, b, c\}$, где $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $c = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$?

Решение. 1) Найдем порядок элемента b: $b^2 = a$, $b^3 = c$, $b^4 = e$. Значит, $O(b) = 4$ и группа A является циклической.

2) По утверждению задачи 7.12 группа A имеет три подгруппы: $\{e\}$, $\{e, b^2\}$, A, т.к. у числа 4 три натуральных делителя: 1; 2; 4.

7.14. ([9], с.188, №1644) Докажите, что для любых элементов a, b, c группы G:

а) элементы ab и ba имеют одинаковый порядок;

б) элементы abc, bca и cab имеют одинаковый порядок.

Решение. а) Пусть $O(ab) = n$, тогда $\underbrace{ab \cdot ab \cdot \ldots \cdot ab}_{n} = e$.

Имеем $a(ba)(ba)\cdot\ldots\cdot(ba) = a, (ba)^n = a^{-1}a = e$. Следовательно, $O(ba) \le n$. $O(ba)$ не может быть меньше n. Если допустить противное, то, аналогично рассуждая, получим, что $O(ab) \le O(ba)$. Следовательно,

$$O(ba) = O(ab).$$

б) 1) $abc = a(bc)$, $bca = (bc)a$; по пункту а) получаем, что

$$O(abc) = O(bca).$$

2) $abc = (ab)c$, $cab = c(ab)$; по пункту а) получаем, что

$$O(abc) = O(cab).$$

3) $O(bca) = O(cab)$ (см. 1) и 2)).

7.15. ([5], с.151, №8.2.18) Вычислите τ^k, если

а) $\tau = \begin{pmatrix} 1234567 \\ 4713526 \end{pmatrix}$, $k = 137$; б) $\tau = \begin{pmatrix} 123456789 \\ 731869452 \end{pmatrix}$, $k = -51$.

Решение.

а) $\tau = (143)(276)$. Легко проверить, что $O((143)) = 3$, $O((276)) = 3$. Тогда $\tau^3 = \varepsilon$, где ε - тождественная подстановка.

$137 = 3 \cdot 45 + 2$, значит, $\tau^{137} = (\tau^3)^{45} \cdot \tau^2 = \tau^2 = (143)^2(276)^2 = (134)(672)$.

б) $\tau = (174856923)$, следовательно, $O(\tau) = 9$. Т.к. $-51 = 9 \cdot (-6) + 3$, то

$$\tau^{-51} = \tau^3 = \tau \cdot \tau^2 = \begin{pmatrix}123456789\\731869452\end{pmatrix}\begin{pmatrix}123456789\\731869452\end{pmatrix}\begin{pmatrix}123456789\\731869452\end{pmatrix} =$$

$$= \begin{pmatrix}123456789\\731869452\end{pmatrix}\begin{pmatrix}123456789\\417592863\end{pmatrix} = \begin{pmatrix}123456789\\874623591\end{pmatrix} = (189)(275)(346).$$

Дополнительные задачи: [8], с.21, №13; [8], с.22, №20; [8], с.22, №21; [8], с.22, №27; [5], с.149, №8.2.1 (остальные пункты); [5], с.149, №8.2.4; [8], с.23, №35; [9], с.189, №1654.

§8. Смежные классы по подгруппе. Теорема Лагранжа

Пусть G - произвольная группа, $Я$ - семейство её подмножеств. На множестве $Я$ можно ввести операцию, а именно, для A и B из $Я$ полагаем

$$AB = \{ab \mid a \in A, b \in B\}.$$

Ясно, что из коммутативности (ассоциативности) операции на G следует коммутативность (ассоциативность) операции на $Я$.

Следующий частный случай умножения подмножеств группы представляет особый интерес.

Определение 8.1. Множество $Hg = H\{g\}$ называется правым смежным классом элемента g по подгруппе H.

Множество $gH = \{g\}H$ называется левым смежным классом элемента g по подгруппе H.

Теорема 8.1. Какова бы ни была подгруппа H группы G, совокупность всех различных правых (левых) смежных классов по подгруппе H образует разбиение группы G.

Задачи

8.1. ([8], с.29, №1) Найдите левое и правое разложение симметрической группы $S_3 = \{p_0, p_1, p_2, p_3, p_4, p_5\}$, где

$$p_0 = \begin{pmatrix}123\\123\end{pmatrix},\ p_1 = \begin{pmatrix}123\\312\end{pmatrix},\ p_2 = \begin{pmatrix}123\\231\end{pmatrix},\ p_3 = \begin{pmatrix}123\\321\end{pmatrix},\ p_4 = \begin{pmatrix}123\\132\end{pmatrix},\ p_5 = \begin{pmatrix}123\\213\end{pmatrix}$$

по её подгруппе $A = \{p_0, p_3\}$. Совпадают ли они между собой?

Решение. Воспользуемся таблицей Кэли для группы S_3 (см. с. 27).

1) Найдем левое разложение: $p_1A = \{p_1 p_0, p_1 p_3\} = \{p_0, p_4\} = A$,

$p_1A = \{p_1p_0, p_1p_3\} = \{p_1, p_5\}$, $p_2A = \{p_2p_0, p_2p_3\} = \{p_2, p_4\}$;

$$S_3 = A \cup p_1A \cup p_2A = \{p_0, p_3\} \cup \{p_1, p_5\} \cup \{p_2, p_4\}.$$

2) Найдем правое разложение: $Ap_0 = \{p_0p_0,\ p_4p_0\} = \{p_0,\ p_4\} = A$,
$Ap_1 = \{p_0p_1,\ p_3p_1\} = \{p_1,\ p_4\}$, $Ap_2 = \{p_0p_2,\ p_3p_2\} = \{p_2,\ p_5\}$;

$$S_3 = A \cup Ap_1 \cup Ap_2 = \{p_0,\ p_3\} \cup \{p_1,\ p_4\} \cup \{p_2,\ p_5\}.$$

3) Левое и правое разложения не совпадают, т.к. $p_1A \neq Ap_1$.

8.2. ([8], с.30, №5) Постройте правое и левое разложения группы G самосовмещений правильного треугольника:
а) по подгруппе M вращений этого треугольника;
б) по подгруппе $A = \{a_0,\ a\}$, где a - одна из симметрий.
Результаты сравнить.

Решение. $G = \{a_0,\ a_1,\ a_2,\ a_3,\ a_4,\ a_5\}$ - группа самосовмещений правильного треугольника. Воспользуемся таблицей Кэли для группы G (см. задачу 4.16).

а) $M = \{a_0, a_1, a_2\}$.

1) $G = M \cup a_3M = \{a_0, a_1, a_2\} \cup \{a_3,\ a_4, a_5\}$.

2) $G = M \cup Ma_3 = \{a_0, a_1, a_2\} \cup \{a_3,\ a_5, a_4\}$.

Левое и правое разложения группы G по подгруппе M совпадают.

б) $A = \{a_0,\ a\}$, пусть $a = a_4$.

1) $G = A \cup a_1A \cup a_2A = \{a_0, a_4\} \cup \{a_1, a_3\} \cup \{a_2, a_5\}$.

2) $G = A \cup Aa_1 \cup Aa_2 = \{a_0, a_4\} \cup \{a_1, a_5\} \cup \{a_2, a_3\}$.

Левое разложение группы G по подгруппе A не совпадают с правым разложением.

8.3. ([8], с.31, №6) Постройте правое и левое разложения группы самосовмещений квадрата по подгруппе $A = \{a_0,\ a\}$, где a - отражение относительно диагонали.

Решение. $M = \{a_0,\ a_1,\ a_2,\ a_3,\ a_4,\ a_5,\ a_6,\ a_7\}$ - группа самосовмещений квадрата; $A = \{a_0,\ a\}$, пусть $a = a_5$. Воспользуемся таблицей Кэли для группы M (см. задачу 4.20).

1) Найдем правое разложение:

$$M = A \cup Aa_1 \cup Aa_2 \cup Aa_3 = \{a_0, a_5\} \cup \{a_1, a_4\} \cup \{a_2, a_7\} \cup \{a_3, a_6\}.$$

2) Найдем левое разложение:

$$M = A \cup a_1A \cup a_2A \cup a_3A = \{a_0, a_5\} \cup \{a_1, a_6\} \cup \{a_2, a_7\} \cup \{a_3, a_4\}.$$

Теорема 8.2. (теорема Лагранжа) Порядок подгруппы конечной группы является делителем порядка группы.

Из теоремы Лагранжа вытекают два следствия.

Следствие 1. Порядок каждого элемента конечной группы является делителем порядка группы.

Следствие 2. Всякая конечная группа, порядок которой есть простое число, не будет иметь собственных подгрупп и является циклической.

8.4. ([8], с.31, №11) Группа содержит 4 элемента, из которых один имеет порядок 4. Какой порядок имеют остальные элементы группы и сколько подгрупп имеет эта группа?

Решение.

1) Пусть $G = \{a_0, a_1, a_2, a_3\}$ - данная группа. $a_0 = e$, $O(e) = 1$.
$O(a_1) = 4$, следовательно, $a_2 = a_1^2$, $a_3 = a_1^3$. Тогда $O(a_2) = 2$, $O(a_3) = 4$, т.к. $a_3^2 = a_1^6 = a_1^2$, $a_3^3 = a_1^2 a_1^3 = a_1$, $a_3^4 = a_1 a_1^3 = e$.

2) Делители 4: 1,2,4. Следовательно, по теореме Лагранжа подгруппы группы G могут иметь порядки 1, 2, 4. Подгруппы группы G будут иметь вид: $\{e\}$, $\{e, a_2\}$, G (см. задачу 7.12).

8.5. ([8], с.31, №12) Сколько подгрупп может иметь группа G, содержащая 17 элементов?

Решение. $|G| = 17$. Число 17 простое, по следствию 2 группа G будет иметь только две подгруппы: $\{e\}$ и G.

8.6. ([8], с.21, №11) Найдите порядок каждого элемента симметрической группы S_3 третьей степени, а затем выясните, какие циклические подгруппы S_3 они порождают. Сколько всего различных подгрупп имеет группа S_3? Является ли A_3 циклической подгруппой группы S_3? Каковы её образующие? (A_3 - знакопеременная группа третьей степени.)

Решение. $S_3 = \{p_0, p_1, p_2, p_3, p_4, p_5\}$.

1) По таблице Кэли для S_3 находим

$$O(p_1) = O(p_2) = 3,\ O(p_3) = O(p_4) = O(p_5) = 2.$$

2) $|S_3| = 6$. Делители 6: 1, 2, 3, 6, следовательно, по теореме Лагранжа, ее подгруппы могут иметь порядки 1, 2, 3, 6. Все подгруппы, кроме S_3, являются циклическими, как группы, имеющие простой порядок 2, 3 (по следствию 2 из теоремы Лагранжа).

Очевидно, $\{p_0\}$ - подгруппа порядка 1; S_3 - подгруппа шестого порядка.

Пользуясь таблицей Кэли, найдем остальные подгруппы.

$\{p_0, p_3\}$, $\{p_0, p_4\}$, $\{p_0, p_5\}$ являются подгруппами второго порядка.

$\{p_0, p_1, p_2\}$ - единственная подгруппа третьего порядка.

Таким образом, группа S_3 имеет 6 подгрупп.

3) $A_3 = \{p_0, p_1, p_2\}$ является циклической подгруппой. У нее два образую-

щих элемента: $A_3 = (p_1) = (p_2)$.

Дополнительные задачи: [8], с.31, №7; [9], с.190, №1659; [9], с.189, №1655.

§9. Нормальные делители и факторгруппы

Как уже было показано, левый и правый смежные классы одного и того же элемента могут не совпадать. Особый интерес, однако, представляет случай, когда эти классы совпадают для каждого элемента группы.

Определение 9.1. Подгруппа H называется нормальным делителем (нормальной подгруппой) группы G, если для всякого элемента $g \in G$ выполняется условие: $Hg = gH$.

Для нормального делителя имеет место равенство $g_1H \cdot g_2H = g_1g_2H$ для любых элементов g_1, g_2 из G. Важность понятия нормального делителя определяется следующей теоремой.

Теорема 9.1. Множество смежных классов группы G по нормальному делителю H образует группу относительно операции умножения классов.

Эта группа называется факторгруппой группы G по нормальному делителю H. Обозначение: G/H.

Иногда бывает удобным пользоваться другим определением нормального делителя. Сформулируем его.

Определение 9.2. Подгруппа H группы G называется нормальным делителем, если $\forall\, h \in H \quad \forall\, g \in G \quad g^{-1}hg \in H$.

Задачи

9.1. ([8], с.33, №4) Докажите, что если порядок подгруппы в два раза меньше порядка самой группы, то эта подгруппа является нормальным делителем группы.

Решение. Пусть G - группа, H - ее подгруппа. $|G| = n$, $|H| = n/2$. Тогда левое разложение группы $G = H \cup gH$, где $g \notin H$, т.к. в классе gH должно содержаться элементов столько же, сколько в подгруппе H.

Таким образом, $gH = G \setminus H$.

Аналогично, правый смежный класс $Hg = G \setminus H$.

Следовательно, $gH = Hg$ и H - нормальный делитель группы G.

9.2. ([8], с.33, №5) Почему в группе самосовмещений квадрата подгруппа поворотов квадрата является нормальным делителем? По-

чему в группе поворотов квадрата подгруппа, порожденная центральной симметрией, является нормальным делителем?

Решение

1) Пусть $M = \{a_0, a_1, a_2, \ldots, a_7\}$ - группа самосовмещений квадрата, а $M_1 = \{a_0, a_1, a_2, a_3\}$ - подгруппа поворотов квадрата.

$|M| = 8$, $|M_1| = 4$, значит, порядок группы M в два раза больше порядка подгруппы M_1. Следовательно, подгруппа M_1 является нормальным делителем группы M.

2) Группа $A = \{a_0, a_2\}$ порождена центральной симметрией квадрата (см. задачу № 4.20). $|M_1| = 4$, $|A| = 2$. Следовательно, A - нормальный делитель группы M_1.

9.3. ([8], с.34, №7) В группе всех самосовмещений квадрата взята подгруппа $H = \{a_0, a\}$, где a - отражение относительно одной из диагоналей квадрата. Является ли H нормальным делителем?

Решение. Пусть $a = a_5$, тогда $H \quad \{a_0, a_5\}$. $a_1^{-1}a_5a_1 = a_3a_4 = a_7 \notin H$ (см. таблицу Кэли задачи 4.20).

Подгруппа H не является нормальным делителем.

9.4. ([8], с.34, №9) Выясните, является ли нормальным делителем группы самосовмещений квадрата ее подгруппа $A=\{a_0, a\}$, где a - отражение квадрата относительно его центра.

Решение. $M = \{a_0, a_1, \ldots, a_7\}$- группа самосовмещений квадрата, по условию $A = \{a_0, a_2\}$ - ее подгруппа.

Тогда $a_1A = \{a_1, a_3\}$, $a_4A = \{a_4, a_6\}$, $a_5A = \{a_5, a_7\}$;

$Aa_1 = \{a_1, a_3\}$, $Aa_4 = \{a_4, a_6\}$, $Aa_5 = \{a_5, a_7\}$

(см. таблицу Кэли задачи 4.20).

Таким образом, $\forall a_i \in M \quad Aa_i = a_iA$, т. е. A - нормальный делитель группы M.

9.5. ([8], с.34, №10) Найдите все нормальные делители в симметрической группе S_3 третьей степени.

Решение.

1) Подгруппами S_3 будут следующие группы:

$\{p_0,\}, A = \{p_0, p_3\}, B = \{p_0, p_4\}, C = \{p_0, p_5\}, A_3 = \{p_0, p_1, p_2\}, S_3$

(см. задачу 8.6).

Очевидно, подгруппы $\{p_0\}$, S_3 являются нормальными делителями S_3.

2) Рассмотрим подгруппу A. $p_1A = \{p_1, p_5\}$, $Ap_1 = \{p_1, p_4\}$, $p_1A \neq Ap_1$.

Подгруппа A не является нормальным делителем.

3) В случае подгруппы B $p_1B \neq Bp_1$, т.к. $p_1B = \{p_1, p_4\}$, $Bp_1 = \{p_1, p_3\}$.

Подгруппа B не является нормальной подгруппой.

4) $p_1C \neq Cp_1$. Подгруппа C не является нормальной подгруппой.

5) $|S_3| = 6$, $|A_3| = 3$. A_3 - нормальный делитель.

9.6. ([8], с.34, №19) Составьте факторгруппу группы Z_8 вычетов по модулю 8 по ее нормальной подгруппе $H = \{\bar{0}, \bar{4}\}$ и таблицу сложения ее элементов.

Решение. $Z_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$, $H = \{\bar{0}, \bar{4}\}$.

1) $\bar{0} + H = \{\bar{0}, \bar{4}\}$, $\bar{1} + H = \{\bar{1}, \bar{5}\}$,
$\bar{2} + H = \{\bar{2}, \bar{6}\}$, $\bar{3} + H = \{\bar{3}, \bar{7}\}$.

Значит, $Z_8 = H \cup [\bar{1} + H] \cup [\bar{2} + H] \cup [\bar{3} + H]$ и
$Z_8/H = \{H, \bar{1} + H, \bar{2} + H, \bar{3} + H\}$.

2) Составим таблицу Кэли для группы Z_8/H:

+	$\bar{0}+H$	$\bar{1}+H$	$\bar{2}+H$	$\bar{3}+H$
$\bar{0}+H$	$\bar{0}+H$	$\bar{1}+H$	$\bar{2}+H$	$\bar{3}+H$
$\bar{1}+H$	$\bar{1}+H$	$\bar{2}+H$	$\bar{3}+H$	$\bar{0}+H$
$\bar{2}+H$	$\bar{2}+H$	$\bar{3}+H$	$\bar{0}+H$	$\bar{1}+H$
$\bar{3}+H$	$\bar{3}+H$	$\bar{0}+H$	$\bar{1}+H$	$\bar{2}+H$

9.7. ([8], с.34, №18) Составьте факторгруппу группы самосовмещений квадрата по ее нормальному делителю $A = \{a_0, a_2\}$ и таблицу Кэли для этой факторгруппы.

Решение

1) $M = \{a_0, a_1, \ldots, a_7\}$ - группа самосовмещений квадрата (см. задачу 4.20), $A = \{a_0, a_2\}$.

Найдем смежные классы, используя таблицу Кэли для группы M:

$$a_1A = \{a_1, a_3\},\ a_4A = \{a_4, a_6\},\ a_5A = \{a_5, a_7\};$$

и тогда M/A $\{A, a_1A, a_4A, a_5A\}$.

2) Составим таблицу умножения для группы M/A, применяя правило умножения смежных классов

$a_1A \cdot a_1A = (a_1a_1)A = a_2A = A$;
$a_1A \cdot a_4A = (a_1a_4)A = a_5A$;
$a_1A \cdot a_5A = (a_1a_5)A = a_6A = a_4A$;
$a_4A \cdot a_1A = (a_4a_1)A = a_7A = a_5A$;
$a_4A \cdot a_4A = (a_4a_4)A = a_0A = A$;
$a_4A \cdot a_5A = (a_4a_5)A = a_3A = a_1A$;
$a_5A \cdot a_1A = (a_5a_1)A = a_4A$;
$a_5A \cdot a_4A = (a_5a_4)A = a_1A$;
$a_5A \cdot a_5A = (a_5a_5)A = a_0A = A$.

Таблица Кэли для факторгруппы M/A:

$\cdot$	A	a_1A	a_4A	a_5A
A	A	a_1A	a_4A	a_5A
a_1A	a_1A	A	a_5A	a_4A
a_4A	a_4A	a_5A	A	a_1A
a_5A	a_5A	a_4A	a_1A	A

9.8. ([8], с.34, №22) Почему подгруппа $A = \{x \mid x = 3k,\ k \in Z\}$ аддитивной группы Z является нормальным делителем группы Z? Каков индекс подгруппы A? Постройте факторгруппу Z/A. Будет ли она циклической? Если да, то каков будет ее образующий элемент и как ее элементы могут быть записаны через этот образующий элемент? (Если число смежных классов (левых и правых) группы G по ее подгруппе H конечно, то это число называется индексом подгруппы H в группе G).

Решение.

1) Аддитивная группа Z коммутативна, поэтому любая ее подгруппа, в том числе и данная подгруппа A, является нормальным делителем группы Z.

2) Найдем смежные классы группы Z по подгруппе A:

$$0 + A = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\} = \overline{0};$$
$$1 + A = \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\} = \overline{1};$$
$$2 + A = \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\} = \overline{2};$$

$Z = A \cup [1 + A] \cup [2 + A]$, индекс подгруппы равен трем.

3) $Z/A = \{A, 1 + A, 2 + A\}$.

Факторгруппа Z/A является циклической с образующим элементом $1 + A$, т.к. $(1 + A) + (1 + A) = 2 + A$,

$$(1 + A) + (1 + A) + (1 + A) = 3 + A = A.$$

9.9. ([8], с.35, №27) Найдите оба разложения знакопеременной группы A_4 четвертой степени по ее подгруппе $V = \{p_0, p_5, p_8, p_9\}$ и сравните результаты. Является ли подгруппа V нормальным делителем группы A_4? Если является, то постройте факторгруппу A_4/V и таблицу умножения ее элементов.

Решение.

Группа A_4 состоит из двенадцати четных подстановок $p_0, p_1, \dots, p_{11}$, где $p_0 = \begin{pmatrix}1234\\1234\end{pmatrix}$, $p_1 = \begin{pmatrix}1234\\1342\end{pmatrix}$, $p_2 = \begin{pmatrix}1234\\1423\end{pmatrix}$, $p_3 = \begin{pmatrix}1234\\2431\end{pmatrix}$,

$$p_4=\begin{pmatrix}1234\\2314\end{pmatrix},\ p_5=\begin{pmatrix}1234\\2143\end{pmatrix},p_6=\begin{pmatrix}1234\\3124\end{pmatrix},\ p_7=\begin{pmatrix}1234\\3241\end{pmatrix},$$

$$p_8=\begin{pmatrix}1234\\3412\end{pmatrix},p_9=\begin{pmatrix}1234\\4321\end{pmatrix},\ p_{10}=\begin{pmatrix}1234\\4213\end{pmatrix},\ p_{11}=\begin{pmatrix}1234\\4132\end{pmatrix}.$$

1) Найдем правое разложение группы A_4 по подгруппе V.

$$Vp_0=V=\{p_0,\ p_5,p_8,p_9\};$$

$$Vp_1=\{p_0p_1,\ p_5p_1,\ p_8p_1,\ p_9p_1\}=\{p_1,\ p_3,\ p_6,\ p_{10}\},\ \text{т.к.}$$

$$p_5p_1=\begin{pmatrix}1234\\2143\end{pmatrix}\begin{pmatrix}1234\\1342\end{pmatrix}=\begin{pmatrix}1234\\2431\end{pmatrix}=p_3;\quad p_8p_1=\begin{pmatrix}1234\\3412\end{pmatrix}\begin{pmatrix}1234\\1342\end{pmatrix}=\begin{pmatrix}1234\\3124\end{pmatrix}=p_6;$$

$$p_9p_1=\begin{pmatrix}1234\\4321\end{pmatrix}\begin{pmatrix}1234\\1342\end{pmatrix}=\begin{pmatrix}1234\\4213\end{pmatrix}=p_{10};$$

$$Vp_2=\{p_0p_2,\ p_5p_2,\ p_8p_2,\ p_9p_2\}=\{p_2,\ p_4,\ p_7,\ p_{11}\},\ \text{т.к.}$$

$$p_5p_2=\begin{pmatrix}1234\\2143\end{pmatrix}\begin{pmatrix}1234\\1423\end{pmatrix}=\begin{pmatrix}1234\\2314\end{pmatrix}=p_4;\ p_8p_2=\begin{pmatrix}1234\\3412\end{pmatrix}\begin{pmatrix}1234\\1423\end{pmatrix}=\begin{pmatrix}1234\\3241\end{pmatrix}=p_7;$$

$$p_9p_2=\begin{pmatrix}1234\\4321\end{pmatrix}\begin{pmatrix}1234\\1423\end{pmatrix}=\begin{pmatrix}1234\\4132\end{pmatrix}=p_{11}.$$

Итак, $A_4=V\cup Vp_1\cup Vp_2$.

2) Найдем левое разложение.

$$p_0V=V=\{p_0,\ p_5,p_8,p_9\};$$

$$p_1V=\{p_1p_0,\ p_1p_5,\ p_1p_8,\ p_1p_9\}=\{p_1,\ p_6,\ p_{10},\ p_3\},\ \text{т.к.}$$

$$p_1p_5=\begin{pmatrix}1234\\1342\end{pmatrix}\begin{pmatrix}1234\\2143\end{pmatrix}=\begin{pmatrix}1234\\3124\end{pmatrix}=p_6,\quad p_1p_8=\begin{pmatrix}1234\\1342\end{pmatrix}\begin{pmatrix}1234\\3412\end{pmatrix}=\begin{pmatrix}1234\\4213\end{pmatrix}=p_{10},$$

$$p_1p_9=\begin{pmatrix}1234\\1342\end{pmatrix}\begin{pmatrix}1234\\4321\end{pmatrix}=\begin{pmatrix}1234\\2431\end{pmatrix}=p_3;$$

$$p_2V=\{p_2p_0,\ p_2p_5,\ p_2p_8,\ p_2p_9\}=\{p_2,\ p_{11},\ p_4,\ p_7\},\ \text{т.к.}$$

$$p_2p_5=\begin{pmatrix}1234\\1423\end{pmatrix}\begin{pmatrix}1234\\2143\end{pmatrix}=\begin{pmatrix}1234\\4132\end{pmatrix}=p_{11},\quad p_2p_8=\begin{pmatrix}1234\\1423\end{pmatrix}\begin{pmatrix}1234\\3412\end{pmatrix}=\begin{pmatrix}1234\\2314\end{pmatrix}=p_4,$$

$$p_2p_9=\begin{pmatrix}1234\\1423\end{pmatrix}\begin{pmatrix}1234\\4321\end{pmatrix}=\begin{pmatrix}1234\\3241\end{pmatrix}=p_7.$$

Итак, $A_4=V\cup p_1V\cup p_2V$.

3) Правое и левое разложения группы A_4 по подгруппе V совпадают. Следовательно, подгруппа V является нормальным делителем группы A_4.

4) $A_4/V=\{V,\ p_1V,\ p_2V\}$.

Составим таблицу умножения для элементов группы A_4/V.

$$p_1V\cdot p_1V=(p_1p_1)V=p_2V,\qquad p_1V\cdot p_2V=(p_1p_2)V=p_0V=V,$$

$$p_2V\cdot p_1V=(p_2p_1)V=p_0V=V,\quad p_2V\cdot p_2V=(p_2p_2)V=p_1V.$$

Таблица Кэли для группы A_4/V:

·	V	p_1V	p_2V
V	V	p_1V	p_2V
p_1V	p_1V	p_2V	V
p_2V	p_2V	V	p_1V

9.10. ([8], с.35, №28) Составьте факторгруппу Z_4/D аддитивной группы Z_4 вычетов по модулю 4 по ее нормальному делителю $D = \{\bar{0}, \bar{2}\}$. Выясните, будут ли Z_4/D и Z_2 изоморфны.

Решение

1) $Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$; $\bar{1} + D = \{\bar{1}, \bar{3}\}$.

Следовательно, $Z_4 = D \cup [\bar{1} + D]$ и $Z_4/D = \{D, \bar{1} + D\}$.

2) Обе группы Z_4/D и Z_2 имеют порядок 2, поэтому они изоморфны (сравните их таблицы умножения).

Определение 9.3. Пусть φ - гомоморфизм группы G в группу G'. Ядром гомоморфизма φ называется множество всех элементов из G, отображающихся в единицу группы G'. Оно обозначается $\mathrm{Ker}\varphi$.

Таким образом, $\mathrm{Ker}\,\varphi = \{g \in G \mid \varphi(g) = e'\}$.

Теорема 9.2. Ядро гомоморфизма является нормальной подгруппой.

Одной из основных теорем теории групп является следующая теорема.

Теорема 9.3. (теорема о гомоморфизмах) Пусть φ - гомоморфизм группы G на группу G'. Тогда факторгруппа $G/\mathrm{Ker}\varphi$ изоморфна группе G'.

9.11. ([9], с.194, №1689) Для мультипликативных групп невырожденных квадратных матриц порядка n доказать утверждения:

а) факторгруппа группы действительных матриц по подгруппе матриц с определителем, равным 1, изоморфна мультипликативной группе действительных чисел, отличных от нуля;

б) факторгруппа группы действительных матриц по подгруппе матриц с определителем равным ± 1, изоморфна мультипликативной группе положительных чисел;

в) факторгруппа группы действительных матриц по подгруппе матриц с положительными определителями является циклической группой второго порядка.

Решение.

а) Как известно, мультипликативная группа действительных невырожденных

квадратных матриц порядка n и ее подгруппа матриц с определителем, равным 1, называются общей линейной группой и специальной линейной группой степени n над полем R соответственно.

Их обозначения: $GL(n,R)$ и $SL(n,R)$.

Зададим отображение φ группы $GL(n,R)$ на группу $R\backslash\{0\}$, полагая для матрицы $A \in GL(n,R)$ $\varphi(A) = \det A$. Ясно, что φ сохраняет операцию умножения. Найдем ядро гомоморфизма φ . Оно состоит из матриц с определителем, равным 1, то есть является группой $SL(n,R)$. По теореме о гомоморфизмах факторгруппа $GL(n,R)/SL(n,R)$ изоморфна мультипликативной группе $R\backslash\{0\}$.

б) Рассмотрим подгруппу $H = \{M \in GL(n,R) | \det M = \pm 1\}$. Полагаем $\varphi(M) = |\det M|$, где матрица $M \in GL(n,R)$, а $|\det M|$ - модуль определителя матрицы M. Отображение φ является гомоморфизмом группы $GL(n,R)$ на группу $R^{|}$. Его ядро совпадает с подгруппой H. Следовательно, по теореме о гомоморфизмах $GL(n,R)/H \cong R^{+}$.

в) Рассмотрим подгруппу $K = \{M \in GL(n,R) \mid \det M > 0\}$ и циклическую группу второго порядка $C_2 = \{1,-1\}$.

Зададим отображение φ, полагая

$$\varphi(M) = \begin{cases} 1, & \textit{если } \det M > 0, \\ -1, & \textit{если } \det M < 0. \end{cases}$$

Отображение φ является гомоморфизмом группы $GL(n,R)$ на группу C_2 и имеет ядро, равное подгруппе K.

Следовательно, $GL(n,R)/K \cong C_2$.

Дополнительные задачи: [8], с.34, №15; [8], с.34, №20; [8], с.34, №21; [8], с.35, №23; [8], с.35, №24; [8], с.35, №25; [8], с.35, №26; [9], с.194, №1689 (остальные пункты); [5], с.159, №8.3.44.

Литература

1. Александров П.С. Введение в теорию групп. Библиотечка “Квант”, выпуск 7. М.: Наука, 1980.

2. Варпаховский Ф.Л., Солодовников А.С., Стеллецкий И.В. Алгебра. М.: Просвещение, 1978.

3. Глухов М.М., Солодовников А.С. Задачник - практикум по курсу высшей алгебры. М.: Просвещение, 1969.

4. Куликов Л.Я. Алгебра и теория чисел. М.: Высш. шк., 1979.

5. Куликов Л.Я., Москаленко А.И., Фомин А.А. Сборник задач по алгебре и теории чисел. М.: Просвещение, 1993.

6. Курош А.Г. Курс высшей алгебры. М.: Наука, 1971.

7. Ляпин Е.С., Айзенштат А.Я., Лесохин М.М. Упражнения по теории групп. М.: Наука, 1967.

8. Нечаев В.А. Задачник - практикум по алгебре. М.: Просвещение, 1983.

9. Проскуряков И.В. Сборник задач по линейной алгебре. М.: Наука, 1984.

10. Шнеперман Л.Б. Сборник задач по алгебре и теории чисел. Минск: Высш. шк., 1982.

Содержание

Учебно-методическое издание

Опорные задачи теории групп: Методическая разработка

Авторы-составители: Ершова Тамара Викторовна,
Карпушина Ольга Геннадьевна

Объем 4,0 п.л. Формат 60×84 1/16
Бумага для множительных аппаратов Заказ
Тираж 100 экз.
454080, Челябинск, пр. Ленина, 69, издательство “Факел”
Челябинского педагогического университета
Типография